cellebrite
delivering mobile expertise

UFED series

UFED Physical Analyzer

User Manual

December 2014

Legal Notices

Copyright © 2014 Cellebrite Mobile Synchronization Ltd. All rights reserved.

This manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Cellebrite Mobile Synchronization Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED Physical Analyzer.
- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Contents

Chapter 1: Introduction 9

1.1. Overview 9

1.2. Physical extraction 10

1.3. Data analysis 12

Chapter 2: Installation and activation 15

2.1. Installing UFED Physical Analyzer 16

2.1.1. System requirements 16

2.1.2. Software installation 17

2.1.3. Activating UFED Physical Analyzer 25

2.1.4. Moving UFED Physical Analyzer with a software license to another PC 32

2.1.5. Enabling connectivity with Windows Vista 35

Chapter 3: Getting started 37

3.1. Starting UFED Physical Analyzer 37

3.2. Link Analysis demo 38

3.3. Opening an extraction for analysis 38

3.4. Opening an extraction in advanced mode 41

3.4.1. Advanced opening of a UFED extraction file 41

3.4.2. Advanced opening of a non-UFED extraction file 52

3.4.3. Saving a .ufd file 64

3.5. Saving a project session 65

3.6. Loading a project session 66

3.7. Closing a project 67

3.8. Closing UFED Physical Analyzer 67

3.9. Keyboard shortcuts 68

Chapter 4: Orientation to the workspace 69

4.1. Project tree 70

4.1.1. Working in the project tree area 82

4.2. Data display area 83

4.2.1. Welcome tab 85
4.2.2. Extraction summary tab 87
4.2.3. Data tabs 89

Chapter 5: Locating and analyzing information 111

5.1. Searching for information in a data tab 111
5.2. Using the quick filter 111
5.3. Using the advanced filter 114
5.4. Searching for information in all open projects 115
5.5. Browsing the file system 116
5.6. Timeline view 117
5.7. Accessing conversation view 120
5.8. Working with watch lists 123
5.8.1. Creating a watch list 123
5.8.2. Editing a watch list 127
5.8.3. Importing a watch list 128
5.8.4. Exporting a watch list 130
5.8.5. Deleting a watch list 131
5.8.6. Running a watch list 132
5.8.7. Locating a watch list 134
5.9. Bookmarking information (entity bookmarks) 134
5.9.1. Creating a new entity bookmark 135
5.9.2. Editing an entity bookmark 136
5.9.3. Deleting an entity bookmark 137
5.10. Device Locations 137
5.10.1. About location data 137
5.10.2. Viewing location data on BING 140
5.10.3. Markers and information windows 143
5.10.4. Retrieving addresses 144

Chapter 6: Translating decoded data 147

6.1. Using the feature 148
6.2. Updating your license with the selected languages 148
6.2.1. Selecting languages in MyCellebrite 148
6.2.2. Downloading the translation pack 154

6.2.3. Translating the decoded data....156
6.2.4. Reporting....158

Chapter 7: Working with project analytics....161

Chapter 8: Scanning for malware....163

8.1. Updating the signature database (online)....164

8.2. Updating the signature database from file (offline)....166

Chapter 9: Generating a report....173

Chapter 10: Performing extractions....183

10.1. Extraction from iOS devices....183
10.1.1. Prerequisites....183
10.1.2. Performing physical extraction....184
10.1.3. Performing advanced logical extraction199

10.2. Extraction from GPS or mass storage devices....210
10.2.1. Reading data from a GPS or mass storage device....213

Chapter 11: Advanced features....217

11.1. Working with TomTom....217
11.1.1. Exporting a TomTom file....218
11.1.2. Importing a TomTom file....219

11.2. Carving images....220
11.2.1. Scanning for carved images....221
11.2.2. Working with carved images....224

11.3. Verifying hash values....224

Chapter 12: Working with hex data....227

12.1. Searching for information in the Hex data and decoded data....230
12.1.1. Searching strings....232
12.1.2. Searching bytes....237
12.1.3. Searching dates....241
12.1.4. Searching SIM ICCID numbers....246
12.1.5. Searching SMS numbers....251

12.1.6. Searching for regular expressions (GREP) ... 255
12.1.7. Searching SMS text strings ... 260
12.1.8. Searching for patterns ... 265
12.1.9. Searching for codes and passwords ... 270
12.2. Browsing the hex extraction ... 274
12.3. Using an offset to jump to a different location in the file ... 275
12.4. Working with bookmarks ... 276
12.4.1. Adding a bookmark ... 276
12.4.2. Editing a bookmark ... 279
12.4.3. Deleting a bookmark ... 279
12.5. Decoding raw data ... 279
12.6. Viewing the hex data information ... 280
12.7. Locating specific data types in the Hex ... 282
Chapter 13: Camera and screenshot evidence ... 283
Chapter 14: Advanced decoding ... 287
14.1. Managing chains ... 287
14.1.1. Constructing a new chain ... 289
14.1.2. Editing an existing chain ... 291
14.1.3. Managing device chains ... 294
14.1.4. Removing a chain ... 300
14.1.5. Chain descriptions ... 300
14.2. Plug-ins ... 304
14.2.1. Managing plug-ins ... 304
14.2.2. Running a specific plug-in ... 306
14.3. Using the Python Shell ... 308
14.4. Exporting the file system ... 309
14.5. Using the Android unlock pattern carver plug-in ... 309
14.6. Android unlock password carver plug-in ... 310
Chapter 15: Settings ... 311
15.1. General settings ... 312
15.2. Data files ... 315
15.2.1. Data files filtering methods ... 316

15.2.2. Managing data files settings 317
15.3. Hex viewer settings 320
15.4. Models settings 322
15.5. Additional report fields 323
15.5.1. Adding a new report field 324
15.5.2. Editing a report field 326
15.5.3. Deleting a report field 326
15.6. Report defaults 326
15.7. Post-chain plugin settings 335
15.8. Saving settings 336
15.9. Loading settings 337
15.10. Setting project settings 337
15.10.1. Setting a unified time zone for the project 337
15.10.2. Setting the case information 341

Chapter 16: Reference 345

16.1. File menu 345
16.2. View menu 346
16.2.1. Viewing the trace window 346
16.3. Tools menu 348
16.4. Extract menu 349
16.5. Python menu 349
16.6. Plug-ins menu 350
16.7. Report menu 350
16.8. Help menu 351

Chapter 1: Introduction

1.1. Overview

UFED is made up of three components:

- The UFED Touch or UFED unit enables logical, password, SIM, file system, and physical extractions from mobile devices, which can then be saved to a USB flash drive, SD memory card, or directly to your PC.
- UFED Physical Analyzer application provides an in-depth view of the device's memory using advanced decoding, analysis, and reports. UFED Physical Analyzer can decode all types of extractions created by the UFED Touch or UFED Classic unit.
- Phone Detective application helps investigators quickly identify a mobile phone by its physical attributes, eliminating the need to start the device and the risk of device lock

The UFED work flow consists of two steps:

- Extraction - Physical, file system, logical, password, SIM card extraction using the UFED Touch or UFED unit
- Decoding, analysis, and reporting using the UFED Physical Analyzer

1.2. Physical extraction

When performing a physical extraction, UFED uses advanced extraction methods to create a single Hex extraction file for each flash memory chip, or address range utilized by the mobile device. Unlike logical extraction processes, the method of the physical extraction is to bypass the device's operating system, and to acquire the data directly from the device's internal flash memory. The device memory is captured into Hex extraction file(s) that are later read and decoded using UFED Physical Analyzer.

The created physical extraction includes memory space unallocated by the device's OS which may contain deleted data such as SMS, call logs, phonebook entries, pictures, videos, and user passwords.

Physical extraction provides a bit-by-bit copy of the entire flash memory of a mobile device. Decoding of physical extractions not only enables the acquisition of intact data, but also data that is hidden or has been deleted. Deleted data can be recovered from files and unallocated space[1].

UFED Physical Analyzer provides advanced carving algorithms, by recovering SQLite records to reveal additional deleted data from unallocated space. The amount of deleted data varies depending on the data on the device. The decoded data is displayed in the same lists as the analyzed data. For example, deleted SMSs from unallocated space are displayed in the same list as the SMSs.

[1] Unallocated space is clusters of a media partition that is not in use for storing active files. It may contain pieces of files that were deleted from the file partition but not removed from the physical disk.

Data carving from unallocated space provides the following benefits:

- Best and quickest solution for uncovering deleted data on the market.
- Additional deleted data in less time.
- Reveals deleted data that was not available previously.
- Higher quality data due to the fact that both false positives and duplicates are automatically removed.
- Automatic activation: There is no need for manual activation.
- Various content types supported such as: SMSs, MMSs, Calls, Contacts, Emails, and application data[2].
- Same view: Ability to arrange all data, including data decoded from unallocated space, in the same views and with timelines.

[2] Application data such as: Kik, WhatsApp, Facebook, Facebook Messenger, Twitter etc.

1.3. Data analysis

UFED Physical Analyzer enables the investigator to perform in-depth analysis of the extracted data and generate reports.

UFED Physical Analyzer has the following key features:

- Decoding of the extraction with a layered view of memory content
    - Provides a detailed view of the Hex file
    - Reconstructs the device file system
    - Decode various Analyzed data types such as: Contact lists, SMS messages, call logs, device information (IMSI, ICCID, user codes), application information, and more
    - Provides a view of data files – images, videos, databases, and so on
    - Provides access to both current and deleted data
    - Reveals device passwords (when applicable)
- Powerful extraction for iOS and GPS devices
- Provides intuitive and user friendly UI for browsing the extracted information
- Powerful analysis and search tools
    - Instant search for all project content
    - Advanced search based on multiple parameters
    - Instant search for data tables content
    - Watch list for highlighting information based on a predefined list of values

    - Time line for viewing all the events performed via the mobile device in a single chronological view
    - Project analytics providing comprehensive activity analysis
    - Malware scanner to identify malware in the device
    - Ability to search the Hex by various parameters such as strings, bytes, numbers, dates
    - Ability to use regular expression search (RegEx) to look for specific data strings
- Ability to bookmark memory locations for indexing of key areas for later review
- Ability to use Python shell commands for data analysis
- Plug-ins
    - Add or remove plug-ins
    - Write your own plug-ins using Python scripting language
    - Manage chains
- Reports
    - Generate reports in various formats
    - Report customizing and personalizing (logo, header, etc.)

Chapter 2: Installation and activation

This chapter describes the installation and activation process of UFED Physical Analyzer on your PC.

2.1. Installing UFED Physical Analyzer

2.1.1. System requirements

PC	Windows compatible PC with a Pentium® IV or compatible processor running at 1.6 GHz or higher		
Operating System	Microsoft Windows XP[3] with SP3 or later Microsoft Windows Vista™, Windows 7 or Windows 8		
Memory (RAM)	OS	Recommended	Minimum
	32 bit	4GB	4GB
	64 bit	8GB	4GB
Space requirements	500 MB of free disk space for installation		
Additional requirements	Microsoft® .Net version 4.0 NOTE: Windows XP 64 bit requires installation of a .Net 2.0 hotfix (NDP20-KB913384-X64.exe) from http://archive.msdn.microsoft.com/KB913384/Release/ProjectReleases.aspx?ReleaseId=771		

[3] By February 28, 2015, the UFED Series will no longer support Windows XP.

Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.

NOTE: To enable extraction to a PC with Windows Vista Operating System, follow the procedure in *Enabling connectivity with Windows Vista* (page *35*).

2.1.2. Software installation

2.1.2.1. Obtaining a copy of UFED Physical Analyzer

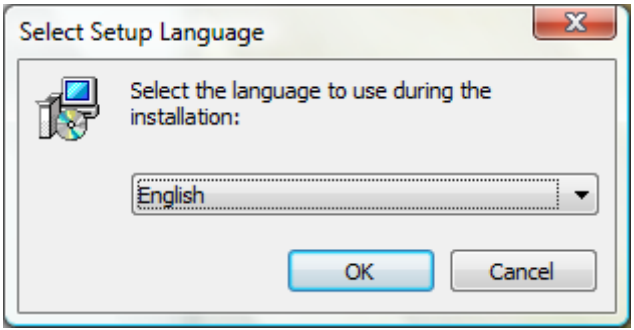
A copy of the latest UFED Physical Analyzer application installer can be obtained from the following sources:

- The UFED Physical Analyzer CD.
- Downloaded from the MyCellebrite site.
- Downloaded from the link provided in the release notes.

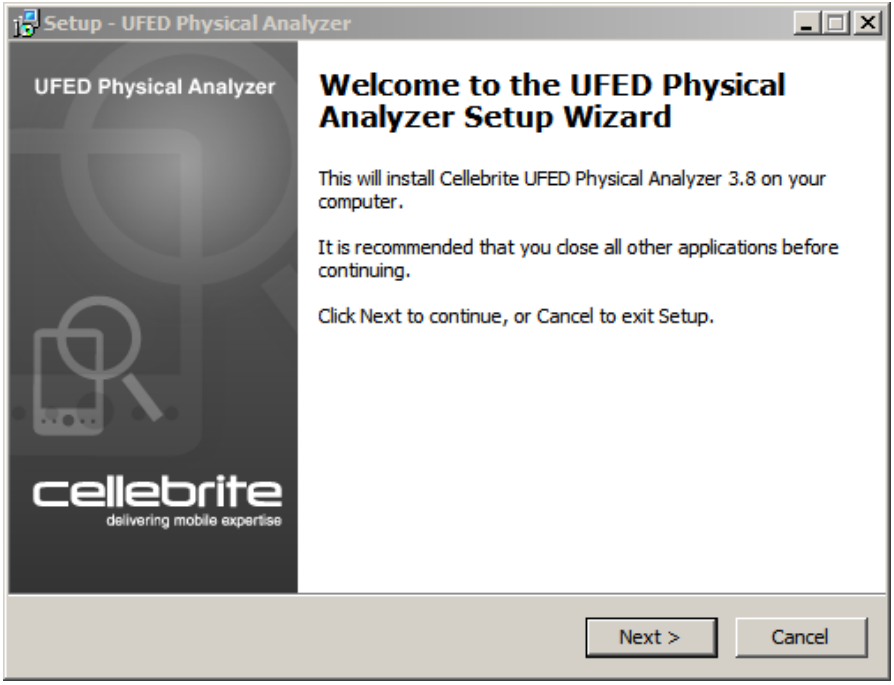
2.1.2.2. Installing UFED Physical Analyzer

NOTE: Before you begin, ensure that cable U-441 is not attached to your computer.

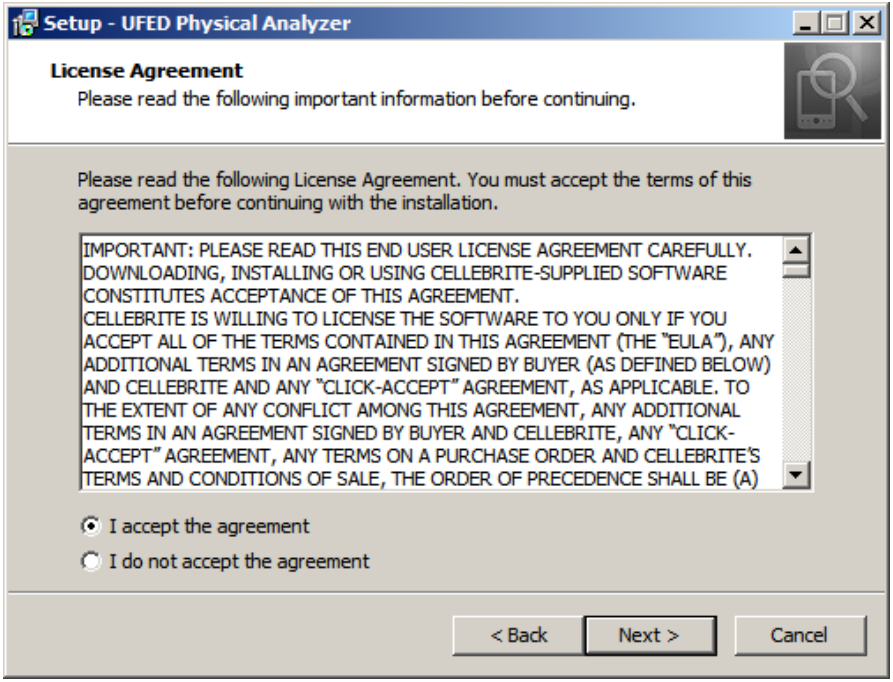
1) Double-click the setup file.



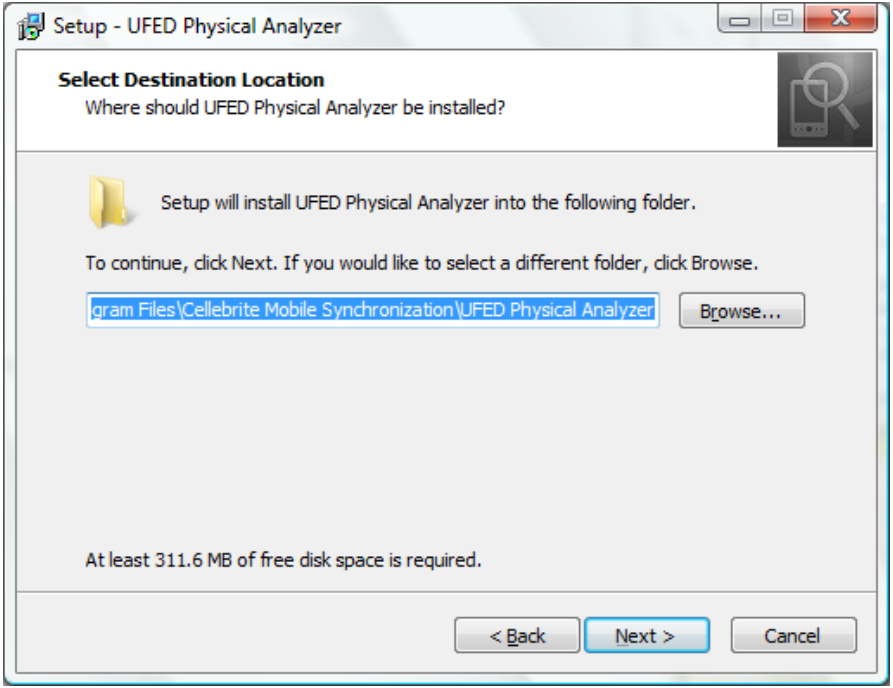
2) Select the desired language and click **OK** to continue.


Setup - UFED Physical Analyzer
UFED Physical Analyzer
Welcome to the UFED Physical Analyzer Setup Wizard
This will install Cellebrite UFED Physical Analyzer 3.8 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
cellebrite
delivering mobile expertise
Next >
Cancel

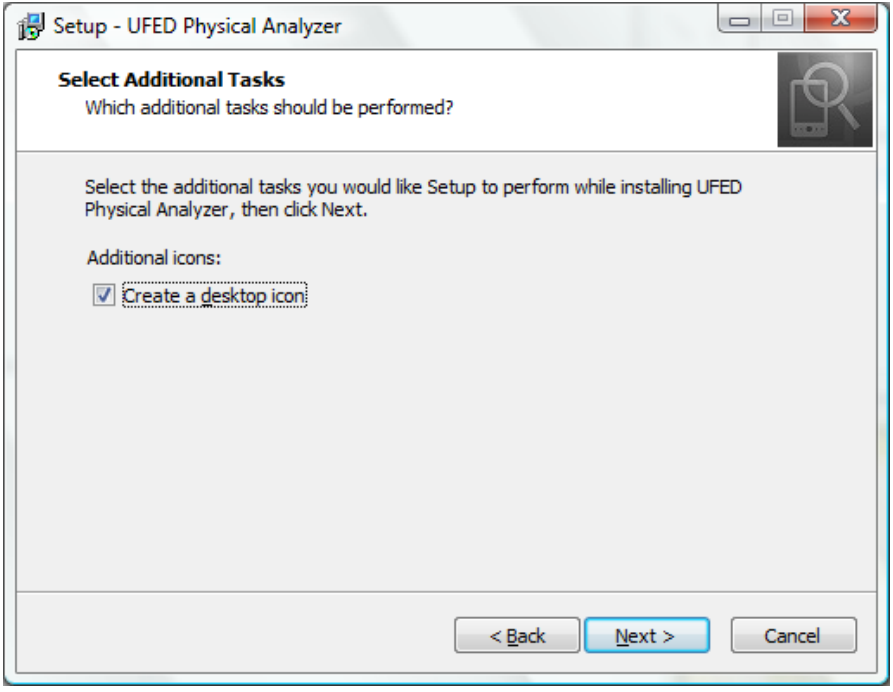
3) Click **Next**.


Setup - UFED Physical Analyzer
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CELLEBRITE-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CELLEBRITE IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS AGREEMENT (THE "EULA"), ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER (AS DEFINED BELOW) AND CELLEBRITE AND ANY "CLICK-ACCEPT" AGREEMENT, AS APPLICABLE. TO THE EXTENT OF ANY CONFLICT AMONG THIS AGREEMENT, ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE, ANY "CLICK-ACCEPT" AGREEMENT, ANY TERMS ON A PURCHASE ORDER AND CELLEBRITE'S TERMS AND CONDITIONS OF SALE, THE ORDER OF PRECEDENCE SHALL BE (A)
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

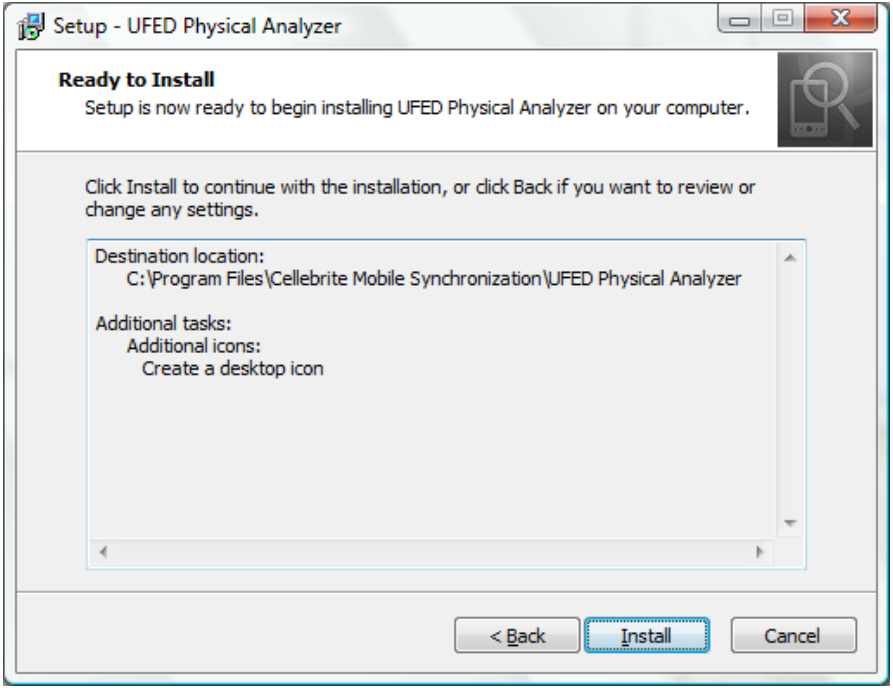
4) Select **I accept the agreement**, and click **Next**.


Setup - UFED Physical Analyzer
Select Destination Location
Where should UFED Physical Analyzer be installed?
Setup will install UFED Physical Analyzer into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
gram Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer
Browse...
At least 311.6 MB of free disk space is required.
< Back
Next >
Cancel

5) If desired, click **Browse** and set a different installation folder.
6) Click **Next**.


Setup - UFED Physical Analyzer
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing UFED Physical Analyzer, then click Next.
Additional icons:
Create a desktop icon
< Back
Next >
Cancel

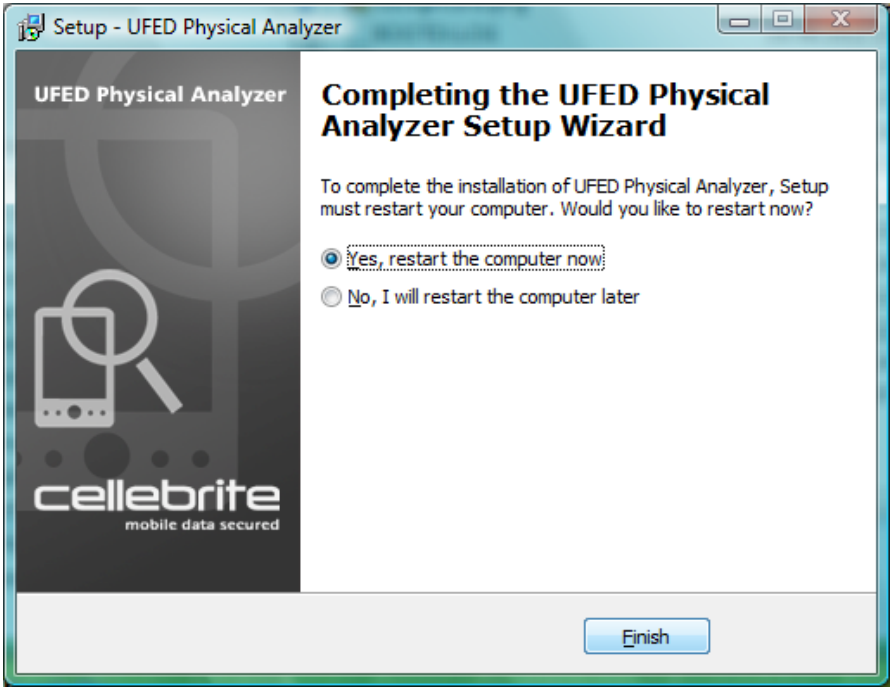
7) If you do not want a desktop icon, clear the **Create a desktop icon** checkbox.
8) Click **Next**.


Setup - UFED Physical Analyzer
Ready to Install
Setup is now ready to begin installing UFED Physical Analyzer on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer
Additional tasks:
Additional icons:
Create a desktop icon
< Back
Install
Cancel

9) Click **Install**.

The installation begins.

NOTE: As part of the installation process, you may be prompted to download and install Microsoft .NET 3.5 Framework. This is part of the installation and requires that your computer has Internet access.


Setup - UFED Physical Analyzer
UFED Physical Analyzer
cellebrite
mobile data secured
Completing the UFED Physical Analyzer Setup Wizard
To complete the installation of UFED Physical Analyzer, Setup must restart your computer. Would you like to restart now?
Yes, restart the computer now
No, I will restart the computer later
Finish

10) Select **Yes, restart the computer now** and click **Finish**.

Your computer restarts and UFED Physical Analyzer is installed.

2.1.3. Activating UFED Physical Analyzer

Activate UFED Physical Analyzer in one of the following ways:

- Using a license dongle
- Using a software license
- Using a network dongle

NOTE: Check your UFED kit to make sure which method you should use.

2.1.3.1. New version notification

Cellebrite will inform you when a newer version of your software is available. If you are connected to the internet you will receive this notification when the new version is available. If you are not connected to the internet the notification will appear every 3 months.

UFED Dongle

2.1.3.2. Using a license dongle

Use the UFED dongle provided with your UFED kit. The dongle contains licenses for all the applications purchased.

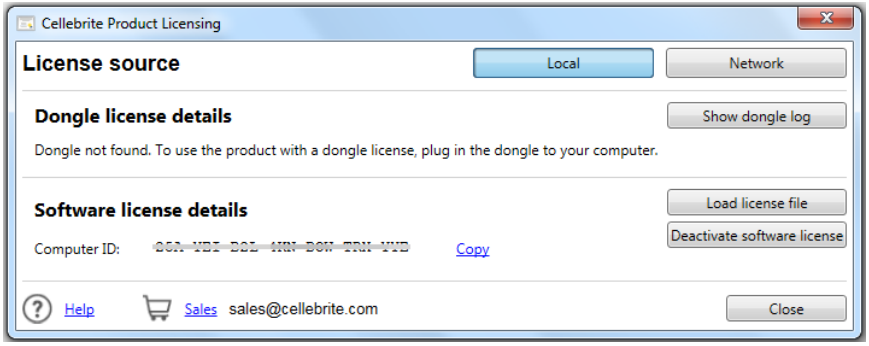
To use UFED Physical Analyzer with a dongle:

1) Connect the dongle to a USB port on your computer. The license is automatically located. When the dongle is recognized by the operating system, the application can read the license.
2) Start UFED Physical Analyzer.

Congratulations, your application is now ready!

If a license dongle is not found:

1) When starting for the first time, or when a license dongle is not found, the Cellebrite Product Licensing window appears.



2) If you connected the dongle to a USB port on your computer, and it still does not work, contact support@cellebrite.com.

NOTE: The HASP dongle drivers must be installed in order to use a hardware license key. If the drivers were not installed during the UFED software installation process, you can run the installation process again and select Install Hasp Dongle Drivers at the end of the process.

2.1.3.3. Using the application with a software license

The first time you open the application, you must activate the license.

To use UFED Physical Analyzer with a software license:

1) Go to the following link: https://my.cellebrite.com/physicalanalyzer
2) Sign into your MyCellebrite account.

   (If you don't have an account, click **Register now**, create a user, and then go back to the required UFED application link.)

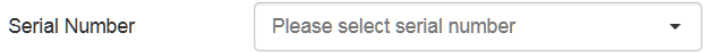
   You will be directed to the product activation window.
3) Click to download the application and save the file to a PC.
4) Extract the zip file, click the installation file and install the software using the Setup Wizard. Restart the PC if required.
5) Repeat step 1 to go to the application link.
6) In the Activation method box, if you purchased UFED 4PC, select **Activation code** or if you purchased UFED Touch, select **UFED Touch/UFED Classic**.

7) Depending on the product you purchased, continue as follows:

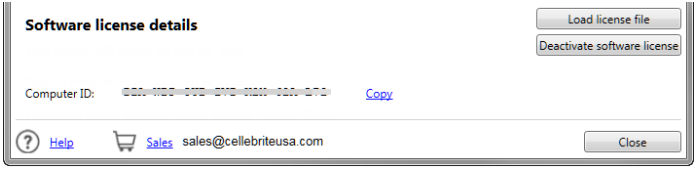
Activation Code

- **UFED 4PC:** In the Activation Code field, enter the Activation code provided with the UFED 4PC kit.

- **UFED Touch:** In the Choose Serial Number field, select the UFED serial number displayed on the UFED Touch unit or UFED Touch License Activation screen.

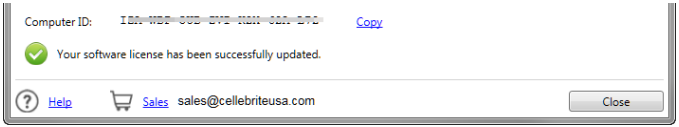
8) Next obtain your Computer ID (do not close the MyCellebrite page while performing this step).
   - Start the application. The Cellebrite Product Licensing window appears.
   - Click **Copy** to copy the Computer ID displayed in the window.



9) In MyCellebrite paste the copied Computer ID.

10) Click **Download Now!** to download your application license key to your PC. The license key will also be sent to your registered MyCellebrite email address.
11) In the application, click **Load license file** in the Cellebrite Product Licensing window.

12) Select the License file and click **Open**. A message appears to indicate that the software license was updated successfully.



13) Click **Close**.

Congratulations, your application is now ready!

2.1.3.4. Using a network dongle

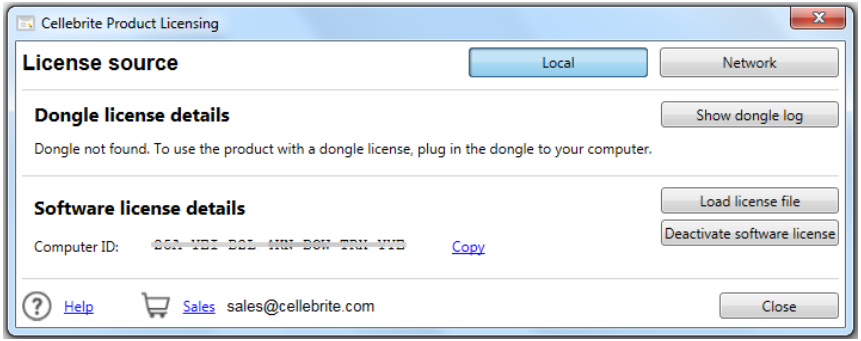
The Network dongle is connected to your organization's network and contains licenses for all the applications purchased.

UFED Network Dongles

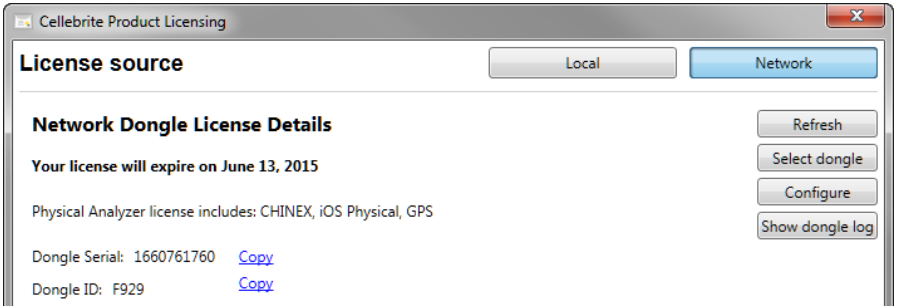
To use UFED Physical Analyzer with a network dongle:

1) Start the UFED application. If the network dongle is connected to the network, the application starts and the user can start working immediately.

   If the network dongle is not recognized, the Cellebrite Product Licensing window appears.



2) Click **Network**. The following window appears.



NOTE: If a dongle was not found on the network – make sure that you have an Internet connection and that a dongle is connected to the network. Then click **Refresh** to search for a network dongle again.

NOTE: By default the network configuration is set to Broadcast. If required, you can manually connect to the network dongle. Click **Configure** to change the network configuration to Specific host. Enter the host name (or IP address) and the port number (1–5 digits).

NOTE: If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required dongle from the list and click **Apply**.

Congratulations, your application is now ready!

2.1.4. Moving UFED Physical Analyzer with a software license to another PC

In cases where a UFED Physical Analyzer installation that has been activated by a software license needs to be moved to another PC, you must first deactivate (remove) the license from the computer. The deactivation process varies between different license versions; follow the instructions in your application.

2.1.4.1. Deactivating version 2 licenses

1) In UFED Physical Analyzer, go to **Help** > **Show License Details**.

   The Cellebrite Product Licensing window appears.

2) Click **Deactivate software license**.

   The Software License Deactivation window appears.

3) Click **Generate deactivation file**.

   UFED Physical Analyzer is deactivated.

4) To get your new UFED Physical Analyzer license, go to **http://my.cellebrite.com/physicalanalyzer**, and follow the license activation steps. For more information, see *Activation using a software license* (page *28*).

2.1.4.2. Deactivating version 5 licenses

1) In UFED Physical Analyzer, go to **Help** > **Show License Details**.

   The Software License Deactivation window appears.

2) Click **Deactivate software license**.

   The Software License Deactivation window appears.

3) Click **Copy** to copy the computer ID.
4) Go to **http://my.cellebrite.com/deactivation**, and log in to your MyCellebrite account.

If you do not have an account, click **Register now** and create a user. Then go back to http://my.cellebrite.com/deactivation.

You are directed to the Deactivation wizard.

5) Paste the copied computer ID, and click **Next**.
6) Click **Download** and download the deactivation file to the PC.
7) In UFED Physical Analyzer, go to **Help** > **Show License Details**.
8) Click **Select Deactivation File**, and select the deactivation file downloaded in step 6.

   Your license is deactivated and UFED Physical Analyzer creates a deactivation file. The Software License Deactivation window informs you that the deactivation file has been created.

9) Return to the Deactivation wizard in MyCellebrite.
10) Click **Choose File**, and upload the deactivation file created by UFED Physical Analyzer.
11) Click **Finish**.
12) To get your new UFED Physical Analyzer license, go to **http://my.cellebrite.com/physicalanalyzer**, and follow the license activation steps. For more information, see *Activation using a software license* (page *28*).

2.1.5. Enabling connectivity with Windows Vista

Perform the following procedure to enable the UFED unit to connect to PCs running the Windows Vista operating system.

1) Go to the Cellebrite Physical Analyzer **Drivers\cbrtucbl** folder.
2) Double-click **USB_Cable_DRV.exe**.
3) Follow the on-screen instructions.

Chapter 3: **Getting started**

UFED Physical Analyzer provides powerful decoding and analysis tools for the extracted device data, and simplifies the task of navigating through the device's data structures. UFED Physical Analyzer assists you in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports.

The application is designed to utilize the memory extracted by the UFED unit and present the device's Hex extraction, file system and analyzed data in a clear and concise way, allowing investigators to use powerful search tools to reveal relevant information.

As a completing step, the application enables you to generate reports of your findings in various file formats, such as HTML, PDF, Excel (*.xlsx), and XML.

3.1. Starting UFED Physical Analyzer

To start UFED Physical Analyzer, do one of the following:

- Double-click the **UFED Physical Analyzer** desktop shortcut.
- Select **Start > Programs > Cellebrite Mobile Synchronization > UFED Physical Analyzer**.

  For an overview of the workspace, see *Orientation to the workspace* (page *69*).

3.2. Link Analysis demo

When you open UFED Physical Analyzer you will be presented with the option to view a sample project in **UFED Link Analysis**.

The UFED Link Analysis demonstration contains preloaded sample content. It consists of 3 reports which have samples of images, SMSs, MMSs and many other pieces of information. The 3 loaded Persons are linked to each other in various ways.

The demonstration has set some Person details, data filters, opened the map tab and created a timeline. All of these are created to show a simple Link Analysis project.

3.3. Opening an extraction for analysis

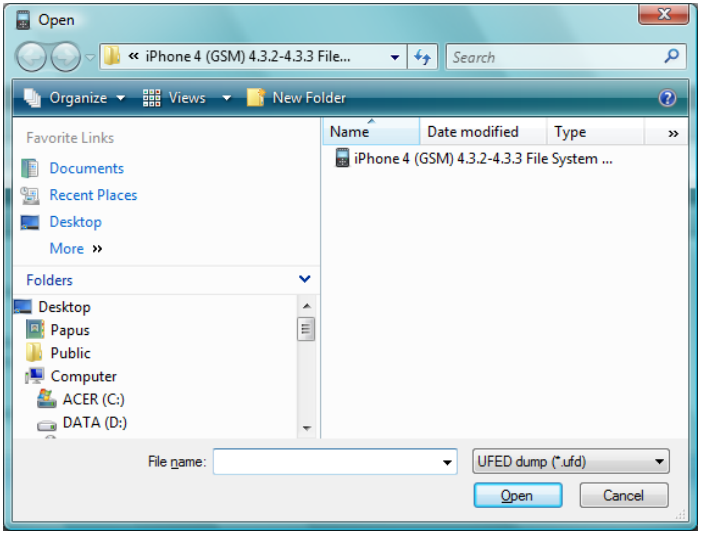
UFED Physical Analyzer can open files created by the UFED device, XML files created by the UFED Physical Analyzer, UFDR files, UFD files and URP files (these files were created in the UFED Report Manager application). In Advanced mode, UFED Physical Analyzer can open image files. For more information, see *Opening an extraction in advanced mode* (page *41*).

1) If the device data was extracted to a removable drive, connect the USB flash drive or SD card containing the extracted data to your PC.

NOTE: For faster processing, copy the extraction folder from the removable media to the PC.

2) Do one of the following:

- In the **Welcome** tab, click **Open**.
- Drag-and-drop the UFD file into UFED Physical Analyzer.
- From the application toolbar, click .
- From the application menu, select **File** > **Open**.



3) Browse to the location of the extracted device data folder and open it.

4) Select an extraction in one of the supported file formats:
    - UFED dump (*.ufd) file
    - Binary files (*.bin). Raw binary files or any Hex extraction generated by another application using the advanced opening feature. See *Opening an extraction in advanced mode* (page *41*).
    - Nokia PM (*.pm)
    - Blackberry backup file (*.ipd)
    - Blackberry backup file (*.bbb)
    - Sony Ericsson GDFS (*.gdfs, *.bin)
    - TomTom CFG (*.cfg)
    - UFED report (*.xml) - Logical reports generated by the UFED unit and XML reports created by the UFED Physical Analyzer
    - UFED Report Manager (*.urp, *.ucp) - UFED Report Pack/UFED Content Pack reports created by Report Manager
    - UFED Report Package (*.ufdr)

    NOTE: By default, the Open dialog box is set to display the *ufd file which is the information mapping file of the extracted device data.

5) Click **Open**.

    The data analysis process (including project analytics) begins and can run for several minutes. At the end of the process, a new project is added to the project tree, and the **Extraction summary** appears in the data display area.

NOTE: To open an extraction quickly when UFED Physical Analyzer is closed, double-click the *.ufd file in the extraction directory. UFED Physical Analyzer opens and begins the data analysis.

3.4. Opening an extraction in advanced mode

The Open (Advanced) feature enables you to specify the device data extraction and decoding options.

Select from two main project opening methods:

- **Select a UFED extraction** - Enables you to specify how to decode a UFED extraction file (*.ufd).
- **Start without a .ufd file** - Enables you to start to decode a physical extraction or a file system that was not generated by a UFED unit.

3.4.1. Advanced opening of a UFED extraction file

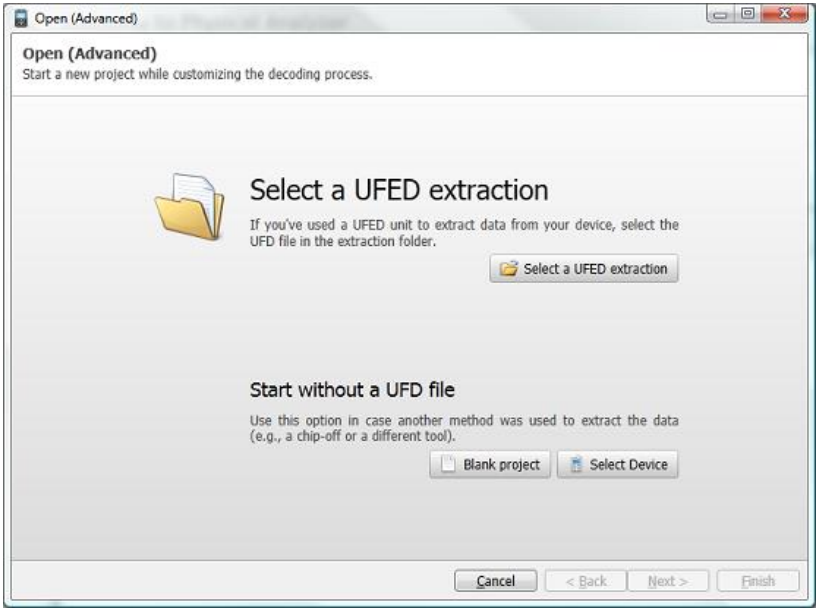
The standard open process activates a decoding process set according to the device and manufacturer information logged in the *.ufd file.

Using the **Select a UFED** extraction method enables you to skip the standard Open process, and specify a custom parsing process, or specify how to parse unknown devices.

To create a new project from UFED extracted data using Open (Advanced):

1) Select **File** > **Open (Advanced)** or click .

   The Open (Advanced) dialog appears, enabling you to set the process of decoding the extracted data for your new project.


Open (Advanced)
Open (Advanced)
Start a new project while customizing the decoding process.
Select a UFED extraction
If you've used a UFED unit to extract data from your device, select the UFD file in the extraction folder.
Select a UFED extraction
Start without a UFD file
Use this option in case another method was used to extract the data (e.g., a chip-off or a different tool).
Blank project
Select Device
Cancel
< Back
Next >
Finish

2) Click **Select a UFED extraction**.
3) In the Open dialog, select the *.ufd file to be processed and click **OK**.

   The dialog contents changes to Advanced Customization and displays the following information detected based on the chosen *.ufd file:

   - **Device** - The manufacturer name and model of the device.
   - **Selected Chain** - The standard device decoding chain automatically assigned to the device.
   - **Binary Dumps** - The binary extractions images referenced by the *.ufd file.

4) Customize the file open options as described in the following sections.
5) Click **Finish.**

3.4.1.1. Specifying a different device

You can specify an entirely different decoding process for the extraction by replacing the selected device.

1) Click **Switch Device**.

2) From the **Select Device** list, select the desired device.
3) To filter the displayed devices, do one of the following:
    - Click on device manufacturer in the list of manufacturers on the left pane
    - Enter the device manufacturer or model in the **Quick Filter** field to filter the displayed devices
4) Click **Next** to return to the Advanced Customization panel.

3.4.1.2. Changing the decoding chain

A chain is a set of plug-ins grouped together in a certain order, which is used to decode the extracted data. Each device in the supported devices list of the application has a predefined decoding chain assigned to it.

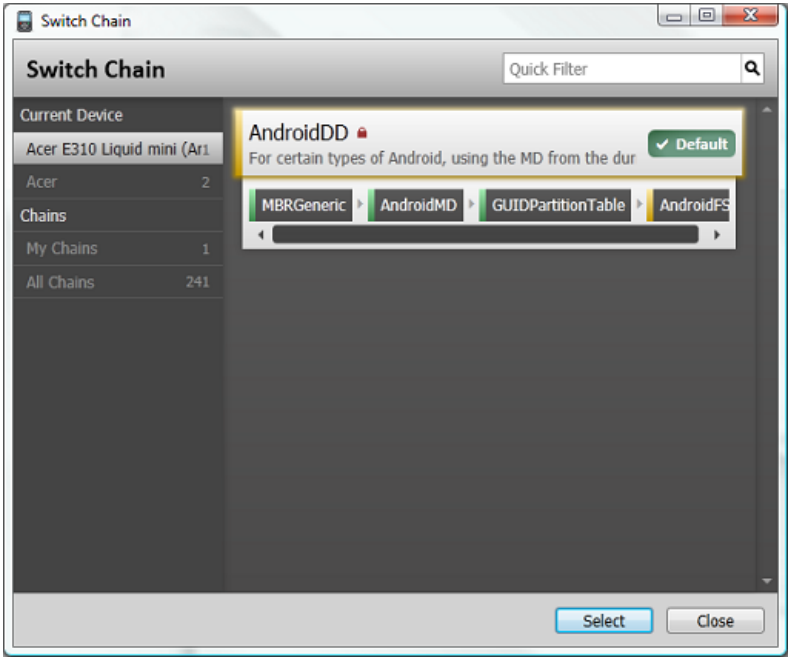
NOTE: Beside plug-ins, a chain can also include other chains, a simpler way to use a predefined set of plug-ins within another chain.

For more information about decoding chains and plug-ins, see *Advanced decoding* (page *283*) and *Plug-ins* (page *304*).

To select a different chain:

1) Click **Switch Chain**.

   The Switch Chain dialog opens and displays the default chain assigned to the device.



NOTE: A device can have several assigned chains, but only one of them can be set as the default chain.

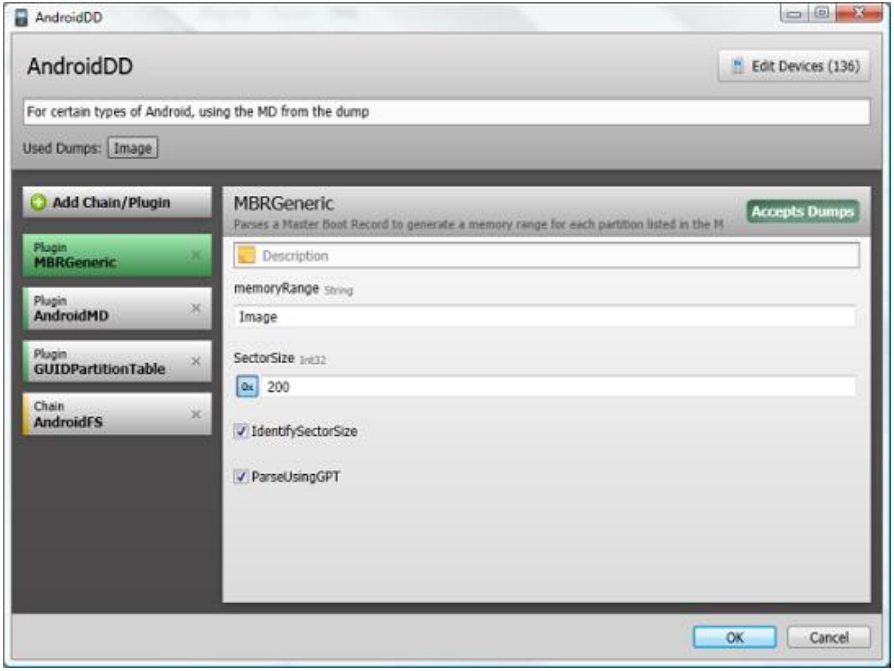
2) From the chains list, select the desired chain in one of the following ways:
   - Select the manufacturer name under the **Current Device** section to display the chains assigned to devices of the same manufacturer.
   - Under the **Chains** section of the list:
     - Select **My Chains** to select from the list of custom chins you constructed.
     - Select **All Chains** to select from the list of all predefined device chains.
     - Use the Quick Filter field to filter the displayed list items.
3) Select the relevant chain, and click **Select** to return to the Advanced Customization panel.

   The default chain is replaced by the selected chain.

To edit the current chain:

1) Click **Edit**.

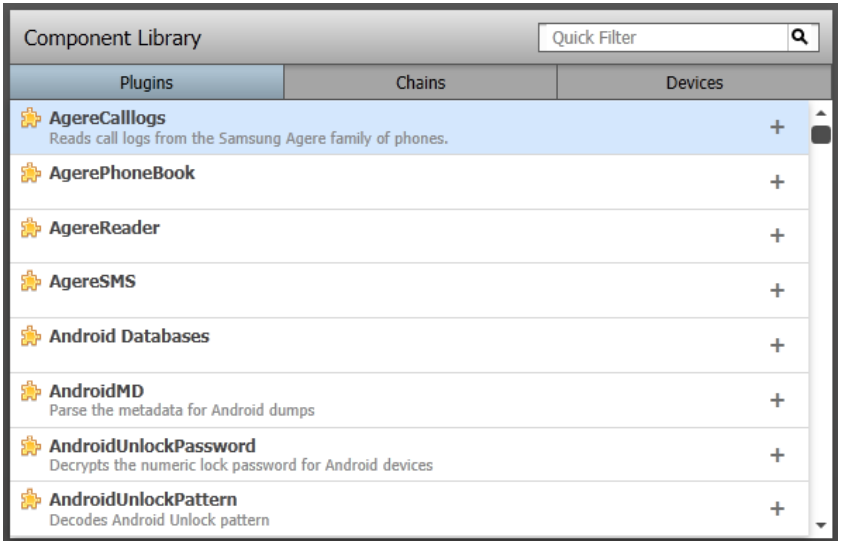
The chain structure dialog of the current chain opens and displays the chain.



2) To add a component to the chain:

   a) Click **Add Chain/Plugin**.

   b) From the **Component Library**, select one of the following:



- **Device**: The entire chain of a specific device.
- **Chain**: A specific predefined chain.
- **Plugin**: A specific plug-in.

NOTE: Items selected under both **Device** and **Chain** are added to the chain as a **Chain component**.

3) Click + to add the component.
4) To remove a component from the chain list, click the x at the right of the component item, then click **Yes** to approve.
5) Click **OK** to return to the Advanced Customization panel.

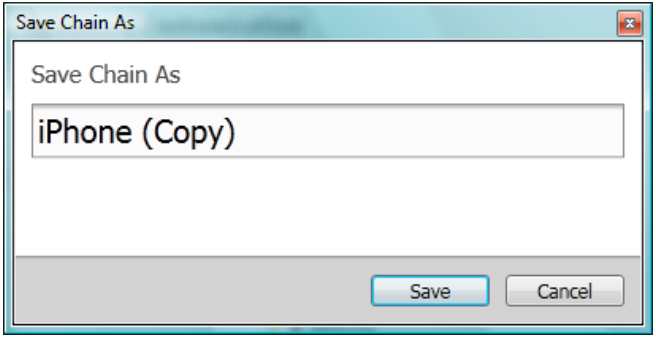
   The default chain is replaced by the customized chain.

To save a customized chain:

After you customize a chain, you can save the changes made to the chain for future use using the **Save As** or **Save** buttons in the **Selected Chain** section.

NOTE: The **Save** button is available only for customizations for unlocked user-defined chains saved in **My Chains**. For more information about user defined chains, see *Managing chains* (page *287*).

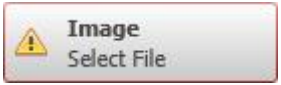
1) Click **Save** to replace the user-defined chain with the current one or **Save As** to save the current chain as a new chain.
2) If you clicked **Save As**, enter a name for the new chain and click **Save**.



The new chain is added to the **My Chains** list of customized chains of the application, and the saved chain appears as the **Selected Chain**.

3.4.1.3. Adding a binary dump

You can add more binary dump files received from a different source.

- To add a binary dump file, click 

or **Add Binary Dump** in the **Binary Dumps** area, and select the binary extraction file you wish to add. Each binary dump you add is shown as a separate component in the **Binary Dumps** section of the dialog.
- To remove a binary dump, click that appears when you position the mouse over it.

3.4.1.4. Adding a file system dump

You can add a file system dump to the project received either as a ZIP archive or as a folder containing the file system extraction files.

- To add a file system extraction, click either **Zip File** or **Folder,** and select the ZIP archive or folder you wish to add.

  NOTE: You can add one file system extraction only. Trying to add more than one removes the previously added file system dump, regardless if it's a zip archive or folder.

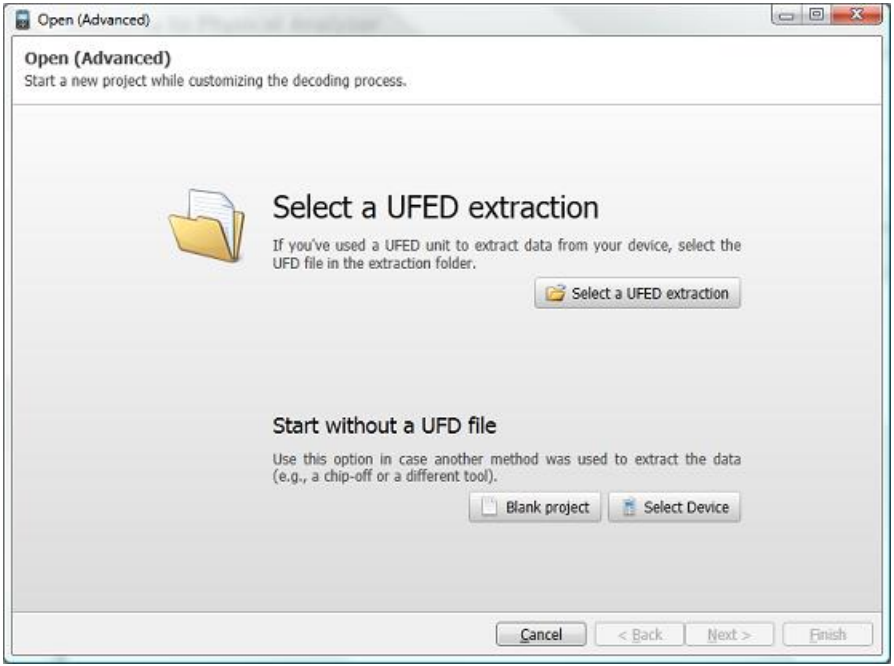
- To remove a file system extraction, click that appears when you position the mouse over it.

3.4.2. Advanced opening of a non-UFED extraction file

When you receive binary or file system extractions that were not generated by a UFED unit, or you don't have the *.ufd file that accompanies them, you can use the Open (Advanced) feature to define how to decode them for the new project.

1) Select **File** > **Open (Advanced)** or click .

The Open (Advanced) dialog appears, enabling you to set the process of decoding the extracted data for your new project.


Open (Advanced)
Open (Advanced)
Start a new project while customizing the decoding process.
Select a UFED extraction
If you've used a UFED unit to extract data from your device, select the UFD file in the extraction folder.
Select a UFED extraction
Start without a UFD file
Use this option in case another method was used to extract the data (e.g., a chip-off or a different tool).
Blank project
Select Device
Cancel
< Back
Next >
Finish

2) The **Start without a UFD file** option provides you with two starting points for your new project:

- **Select Device** - Select the specific device definition to use to decode the data extraction. This option is useful when the device manufacturer and model are known to you. See *Starting with device selection* (page *54*).
- **Blank Project** - Provides you with an empty **Advanced Customization** panel to set your process parameters and data. This option is useful when you have no information about the device and/or manufacturer, and would like to construct a custom decoding process. See *Starting from a blank project* (page *56*).

3.4.2.1. Starting with device selection

Create a new project for data extraction based on a known device.

1) In the Open (Advanced) window, click **Select Device**.

2) From the **Select Device** list, select the desired device.
3) Use the list of manufacturers on the left to filter the displayed devices by manufacturer, and the **Quick Filter** field to filter the displayed devices by any string.
4) Click **Next**.

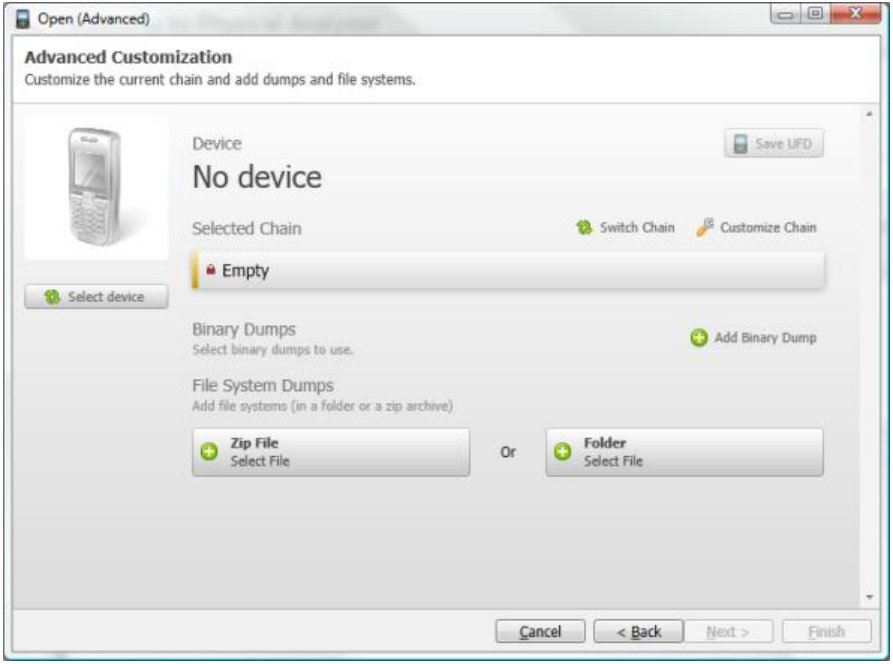
The Advanced Customization panel displays the name and default decoding chain of the selected device.

- To select a different device, see *Specifying a different device* (page *44*).
- To select a different parsing chain, see *Selecting a different chain* (page *46*).
- To customize the parsing chain, see *Editing the current chain* (page *47*).
- To add binary extractions, see *Adding a binary dump* (page *51*).
- To add a file system extraction, see *Adding a file system dump* (page *52*).

5) Click **Finish**.

3.4.2.2. Starting from a blank project

1) In the Open (Advanced) window, click **Blank project**.



2) To select a device, see *Specifying a different device* (page *44*).
3) To select a parsing chain, see *Selecting a different chain* (page *46*).
4) To customize the parsing chain, see *Editing the current chain* (page *47*).

5) To add binary extractions, see *Adding a binary dump* (page *51*).
6) To add a file system extraction, see *Adding a file system dump* (page *52*).
7) Click **Finish**.

3.4.2.3. JTAG extractions

JTAG (Joint Test Action Group) is an advanced method of data extraction that requires a forensic examiner to connect to the test access ports of the device to obtain a full physical image. This enables the examiner to unlock and gain access to the raw data stored on the memory chip.

JTAG is non-destructive and offers the opportunity to access data from devices that have been altered or damaged in some, where data ports are unavailable (or disconnected), or it is otherwise impossible to unlock the device using other forensic tools.

UFED Physical Analyzer automates the JTAG decoding process and saves you time in that you no longer need to manually decode the large volume of raw data found in JTAG extractions. The following table displays a sample list of some of the supported devices:

Vendor	Model
Casio	C711 GzOne Boulder C751 GzOne Ravine
HTC	A7272 Desire Z Google Nexus One
Huawei	M860 Ascend Ascend Y300 (Android)
Kyocera CDMA	S2100 S2300 Torino (CommonCents)
LG CDMA	LX-290 VS-740 Ally
Nokia	Lumia 520 Lumia 920
Pantech	Razzle TXT8030VW (Verizon Wireless) Renue P6030
Samsung GSM	SGH-i337 Galaxy S4 SGH-i437 Galaxy Express
Sanyo CDMA	SCP-2700 Juno
T-Mobile	Touch Pro 2
ZTE GSM	Z221

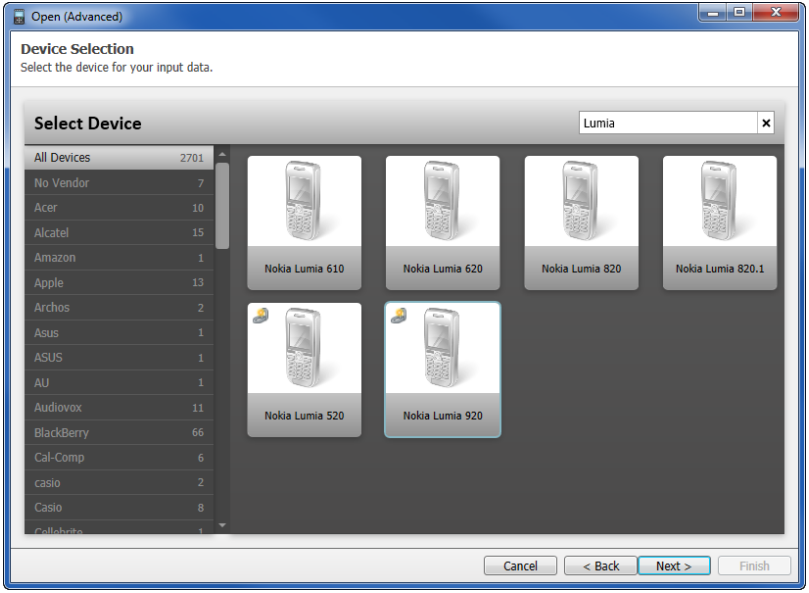
For an updated list of devices that support JTAG extractions, refer to the UFED Phone Detective Mobile App or http://www.cellebrite.com/mobile-forensics/support/ufed-supported-devices.

Once you have the physical memory that was acquired with this method, you can load it into the UFED Physical Analyzer for decoding. When loading the appropriate UFED JTAG chain, you will receive all the data, as if it was a regular extraction.

The main difference between a JTAG extraction and a UFED extraction are the locations of "spares" inside the extraction. Spares are the technical term for metadata of blocks inside the extraction. They can be located in several locations inside the extraction. In regular extractions, they are located at the end of each block. In JTAG extractions they are located at the end of the extraction.

To decode the data extraction using JTAG:

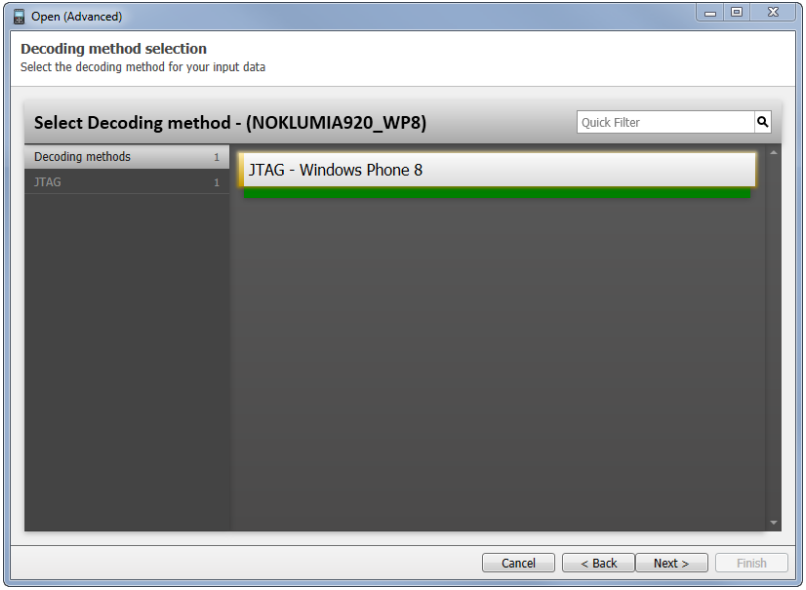
1) In the Open (Advanced) window, click **Select Device**.
2) To filter the displayed devices, enter the device manufacturer or model in the **Quick Filter** field, or click on device manufacturer in the list of manufacturers on the left pane.



NOTE: If JTAG is not supported for the required device you can enter "jtag" In the Quick Filter field to select a generic JTAG device.

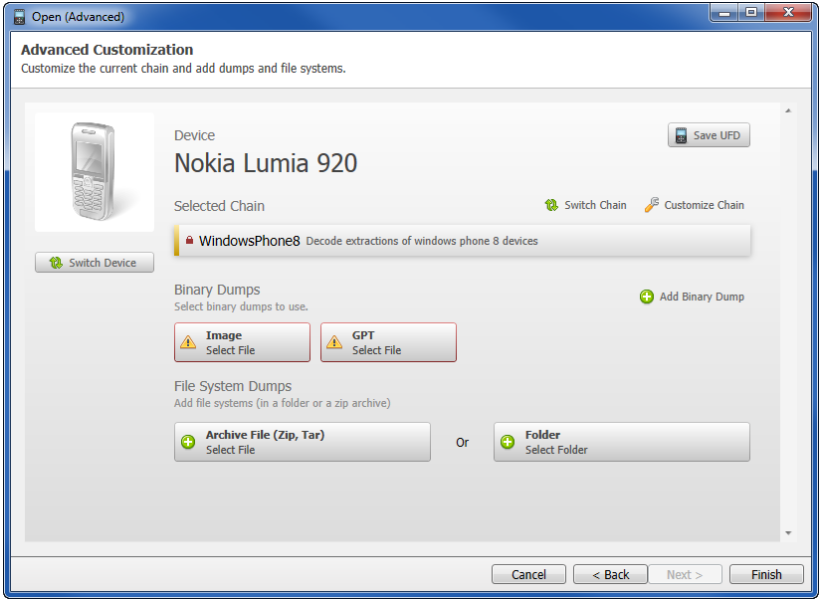
3) Select the required device and click **Next**.

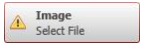
The following window is displayed.



4) Select the decoding method and click **Next**. The available methods change from device to device.

The following window appears.



5) To add a binary dump file, click 

or **Add Binary Dump** in the **Binary Dumps** area, and select the binary extraction file you wish to add. Each binary dump you add is shown as a separate component in the **Binary Dumps** section of the dialog.

6) Click **Finish**.

3.4.3. Saving a .ufd file

At any point of setting the Open (Advanced) parameters, you can click **Save UFD** at the top right corner of the dialog to save a *.ufd file that logs the selected binary extractions and device information for future use.

The next time you need to decode that file, you can use the saved UFD file to open it with **Open** or **Open (Advanced)**.

3.5. Saving a project session

Save the project session to save your work on the project, enabling you to close UFED Physical Analyzer and restart your session at a later time.

The saved session file (.pas) includes:

- User selection in the Analyzed Data and Data Files tables
- Hex bookmarks
- Entity bookmarks
- Watch list results
- Opened tabs
- Generated reports

A project session can also be created for extractions performed by third party tools.

NOTE: Saved project sessions do not contain defined settings. For more information on how to save your settings, see *Saving settings* (page *336*).

To save a project session:

1) In the **File** menu, select **Save Project Session**.

   The Save As dialog box appears.

2) Browse to the location where you want to save the project session file.
3) To change the file name, edit the automatically assigned name in the **File name** box.

   NOTE: To overwrite an earlier session, choose the same file name.

4) Click **Save**.

3.6. Loading a project session

1) From the **Welcome** tab, open the project that you want to work in.
2) In the **File** menu, select **Load Project Session**.
3) In the Open dialog box, browse to and select the project session file that you want to open.
4) Click **Open**.

   The session opens.

3.7. Closing a project

- Do one of the following:
    - In the **File** menu, select **Close**.
    - Right-click the project name and select **Close**.

3.8. Closing UFED Physical Analyzer

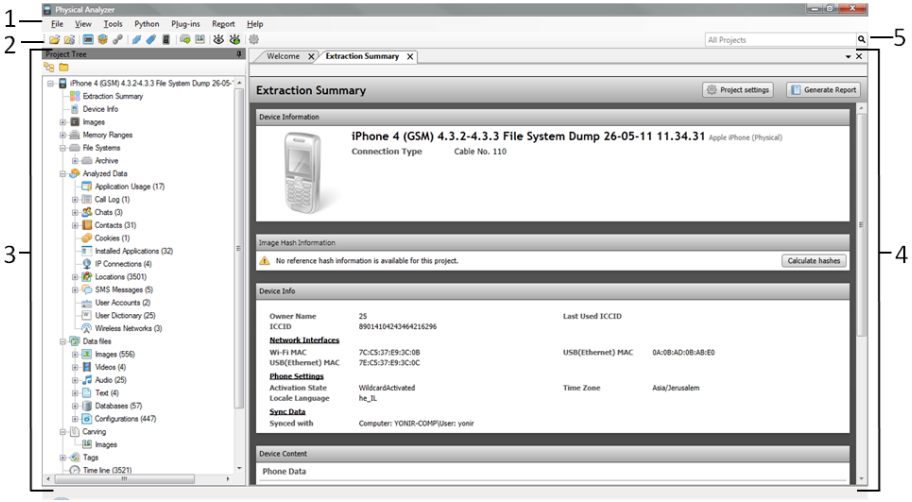
- In the **File** menu, select **Exit**.

3.9. Keyboard shortcuts

Ctrl+O	Open a file
Ctrl+W	Close a project
Ctrl+P	Open project settings
Ctrl+Shift+O	Open advanced
Ctrl+I	Open iOS wizard
Ctrl+T	Open settings
Space	Select or clear check boxes
Ctrl+R	Open the report wizard
Ctrl+Tab	Switch between open tabs
Ctrl+Home	Move the cursor to the beginning of a table
Ctrl+End	Moves the cursor to the end of a table
Ctrl+B	Add an entity bookmark
Ctrl+J	Extract GPS or mass storage device
Ctrl+U	Open the UFED Downloader to connect to UFED
Ctrl+D	Select a folder for the dump file system

Chapter 4: **Orientation to the workspace**

The workspace contains two main areas; the project tree and the data display area to streamline your workflow.



The workspace contains the following components:

1) Application menu bar
2) Application toolbar
3) Project tree
4) Data display area
5) All projects search

4.1. Project tree

The **Project Tree** area displays the following extracted information structure of each project opened for analysis:

Tree item	Description
Extraction Summary	• Double-click **Extraction Summary** to open a summary of the project in the data display area. For more information, see *Extraction summary tab* (page *87*).

Tree item	Description
Device Info	• Double-click **Device Info** to open a tab in the data display area. The **Device Info** tab provides a list of existing information, as well as important identifiers for the device, such as SIM card and user lock codes, where supported. The number of categories and amount of displayed information depends on the device model and manufacturer.
Images	• Double-click an image item to display it in a Hex View tab in the data display area. The **Images** tree item lists all the extraction files generated from the memory modules of the device.

Tree item	Description

Memory Ranges	The **Memory Ranges** tree item lists the analyzed memory ranges for each of the extracted memory module of the device (listed under **Images**).
	• Select a memory range to:
	  ◦ Highlight the memory range portion in the displayed data
	  ◦ Add it to the highlights list of the displayed binary image it belongs to (located at the bottom of the Hex view tab).
	• Double-click a memory range item to display its content in a new Hex view tab.

Tree item	Description
File Systems	The **File Systems** tree item lists all the file systems found or reconstructed out of the analyzed binary file. Each file system is marked with (hard drive). Deleted files are marked with (red cross). • Double-click any file system item to display its content in a new Hex view tab.

Tree item	Description
Analyzed data	The **Analyzed Data** tree item displays groups of analyzed data that are related to device-specific features such as contacts, SMS messages, call logs, and so on. The available information and what is displayed depends on the device features and application version. For example, SMS messages are sorted according to the folders used by the messaging feature of the device, such as Drafts, Inbox, Outbox, Sent, and so on. Email messages are sorted according to the account through which they were sent or received. An uncategorized account or messages folder lists the folders or messages that cannot be categorized in any of the found accounts or account folders (Inbox, Outbox, Drafts, and so on). The following information types may be displayed in **Analyzed Data**: • Personal information - Calendar, contacts, notes, call log, user dictionaries, user accounts • Messaging items - SMS, MMS, email, instant messages, chat

Tree item	Description
	• Web browser items - Bookmarks, history, cookies • GPS information - Locations (including from video files, metadata, and SQLite databases), journeys, fixes. For more information on geolocations, see *About location data* (page *137*). • Device information - Bluetooth pairings, wireless networks, SIM data, application usage, Wi-Fi, cellular locations The number in parenthesis designates the number of items each category contains. Selecting any analyzed data category automatically adds it to the highlights list of the displayed binary image and/or memory range it belongs to (located at the bottom of the Hex view tab), and highlights its data range portions in the displayed data.
Data files	The **Data Files** tree item sorts the extracted data into common or known file formats, used by devices and computers, such as images, videos, audio, text, or document files.

Tree item	Description
	In the project tree, the information is displayed in the following categories: • **Images** - Files that were recognized as image file formats • **Videos** - Files that were recognized as video file formats • **Audio** - Files that were recognized as audio file formats • **Text** - Files that were recognized as text file formats • **Databases** - Data structures that were recognized as databases • **Configurations** - Device configuration files (such as iOS plist files) • **Applications** - Files that were recognized as application files (such as .apk, .jar, .dex, .so, .exe files etc.) • **Documents** - Files that were recognized as document file formats (such as .doc, .docx, pdf; xlsx, ppt files etc.) Deleted items are marked with (red cross).

Tree item	Description
	You can create additional data file groups. For more information, see *Managing data files settings* (page *317*).
Carving	The **Carving** tree item enables you to search the physical extraction for partially deleted or corrupted images. • Double-click **Carving** to start the search. For more information, see *Carving images* (page *220*).
Tags	Certain file types are identified and tagged in the extracted data. There are eight default tags: **Applications**, **Audio**, **Configurations**, **Databases**, **Documents**, **Images**, **Text**, and **Videos**. You can use plug-ins or the Python shell to look for additional data segments and tag them with one of the existing tags, or with a custom tag. Deleted items are marked with (red cross).

Tree item	Description
Timeline	• Double-click **Timeline** to open the device events organized by time in the data display area. The **Timeline** tab displays the device's time stamped events, such as calls, SMS, MMS, and so on, in chronological order.
Watch lists	Watch lists are lists of keywords that you create and then use to search and identify events and items of interest in the extracted data. • Expand **Watch Lists** to view a list of watch lists that have been run in the current session. • Double-click on **Watch Lists** to view the highlighted entity based on the watch lists. For more information, see *Working with watch lists* (page *122*).

Tree item	Description
Bookmarks	The bookmarks that you create to define and save specific locations in the Hex data are managed in the **Bookmarks** tree item. • Double-click **Bookmarks** to open a bookmarks list in a tab in the data display area.

Tree item	Description
Entity bookmarks	The entity bookmarks you create are managed in the **Entity Bookmarks** item of the project tree. The number of entity bookmarks in the project is shown in brackets next to the section name. • Double-click **Entity Bookmarks** to list the entity bookmarks in a tab in the data display area. • Double-click any entity bookmark to go to the bookmarked item in the appropriate display tab. For example, double-click an entity bookmark to an SMS message to open the list of SMS messages in an Analyzed Data display tab, with the bookmarked item highlighted. For more information, see *Bookmarking information (entity bookmarks)* (page *134*).

Tree item	Description
Reports	To open a report that has already been generated for the project: • Double-click the report in the **Reports** tree item. The report opens in the application associated with the report format. • If no reports have been generated for the project, double-click the **Reports** tree item to open the Generate Report dialog box. For more information on generating a report, see Generating a report.
Malware Scanner	Run the malware scanner to identify malware on the device. For more information, see *Scanning for malware* (page *163*).

Tree item	Description
Project Analytics	The **Project Analytics** tree item provides you with a comparative analysis overview. You can open an Activity Analytics tab showing an overview of all device activity, as well as tabs that each focus on the phone, email, WhatsApp, Skype, Gmail, and BlackBerry Messenger activities. For more information, see *Setting project settings* (page *337*).

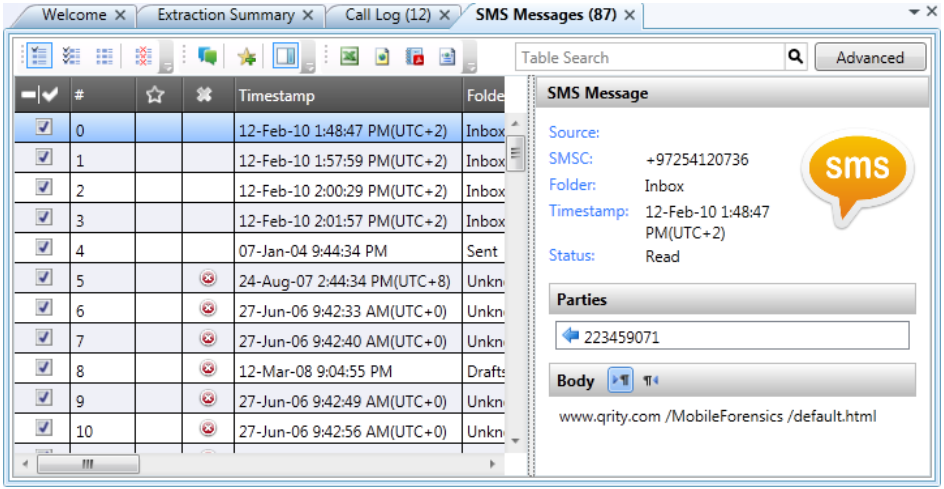
4.1.1. Working in the project tree area

Open the tree items to drill down and locate specific information:

- Click to expand or to collapse tree items.
- Double-click a tree item to open detailed information in the data display area.
- Click at the top of the project tree to expand all the items in the tree.
- Click at the top of the project tree to collapse all the items in the tree.

4.2. Data display area

Double-click an item to display it in a tab. A new tab is opened for each item.



There are five tab types:

- **Welcome** tab
- **Extraction Summary** tab
- **Data** tabs, with sub-tabs that present a particular view, depending on the data
- **Timeline** tab
- **Image** tab (Hex view)

The data display area also displays additional windows such as the Trace window, and Watch list results.

To close a tab:

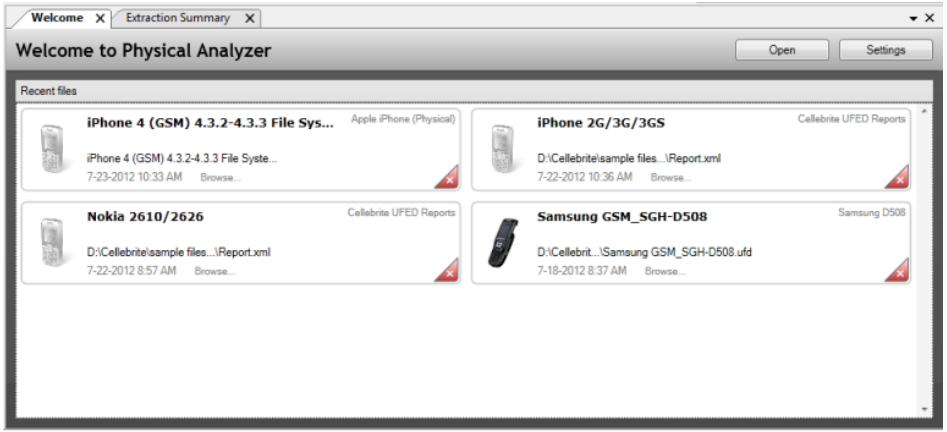
- Do one of the following:
    - Click ✕ on the tab header.
    - Click ✕ at the top right of the data display area.

To jump to a specific tab

- At the top right of the data display area, click ▾, and select the desired tab from the open tabs list.

4.2.1. Welcome tab

The **Welcome** tab is automatically displayed in the data display area when the application is launched and displays a list of recently opened files.



Each file in the list is displayed as a framed information group that contains the following items:

- Device picture - A thumbnail image of the device from the application resources, if available. When unavailable, a general placeholder image is used.
- File name - The name of the opened file, without the file extension.

- File path - The file system path to the file location.
- Device model - The identified device manufacturer and model, or BINARY if the opened file was a binary extraction.
- Case name - If the report was given a case name, the name is shown. The name can be defined in the project settings.
- Date and time - The date and time stamp in which the file was last opened.
- Browse link - A direct link to the file in the system.
- Remove recent item - Click to remove the item from the **Welcome** tab.

You can do the following:

- Click on a framed item to open the files for decoding.
- Click **Browse** to go directly to the file associated with it in the file system.
- Close the **Welcome** tab. To reopen it, go to **View** > **Show Welcome**.

4.2.2. Extraction summary tab

The **Extraction Summary** tab is displayed automatically whenever you open a new extraction for analysis.

- To reopen the tab if closed, double-click the **Extraction Summary** tree item.

The **Extraction summary** tab can display the following information:

- **Extraction Info** - Information related to the device extraction. Such as:

Extraction start date/time *Extraction end date/time*	When the extraction started and ended.
Unit Identifier	The serial number of the device that performed the extraction (e.g., UFED Touch), or a unique ID if the extraction was performed by a PC application (e.g., UFED 4PC).
Unit Version	UFED software version (e.g., 4.1.0.220)
Selected Manufacturer	Manufacturer of the device (e.g., Apple)
Selected Device Name	Device name (e.g., iPhone 4)
Connection Type	Cable used for the extraction (e.g., Cable No. 100)
Extraction Type	Type of extraction performed (e.g., File system)
Extraction ID	Unique ID for each extraction type

- **Image Hash Information** - Verification of the logged hash values of the parsed images. See *Verifying hash values* (page *224*).
- **Device Info** - A summary of the specific device info pulled from the extraction file. See the *Device Info* item in *Project tree* (page *70*).
- **Device Content** - Analyzed content, divided into the following categories:
    - **Phone Data** - The types of analyzed device data found in the extraction, such as call log, contacts, SMS messages, and so on. For the complete list of phone data types, see the *Analyzed Data* item in *Project tree* (page *70*).
    - **Data Files** - The types of standard data files found in the extraction, such as images, videos, audio, and text files. See *Data files* (page *315*).

To display the relevant information in a new tab in the data display area:

- Click any of the tree items.

4.2.3. Data tabs

Data tabs show files of a specific type (such as call log, contacts, SMS messages, and so on).

Each type of data file has several data display modes:

Application files	**Hex View** and **File Info**
Image files	**Hex View**, **Image View** and **File Info**
Video files	**Hex View**, **File Info** and **Video View**
Audio files	**Hex View** and **File Info**
Text files	**Text View, Hex View** and **File Info**
Document files	**Hex View** and **File Info**
Databases	**Database View**, **Hex View**, and **File Info**
Configurations	**Hex View** and **File Info**

Data tabs display the data in a variety of sub-tabs, depending on the data type:

- **Table view** - A list of all the files of a specific type (images, videos, audio, text, and so on) that were found during the data analysis process.
- **Folder view** - View the folder structure of the data files paths in the reconstructed file system (for data files only).
- **Hex view** - View the Hex data of a binary item
- **Image view** - View the image. See *Viewing image files* (page *108*).
- **Thumbnail view** - View images by thumbnail (for images only).
- **File Info** - View information about the file.
- **Database view** - View the contents of database files.

4.2.3.1. Working in data tabs

Selecting items

Select items in the data display area to include them in any report you generate. By default, all items are selected.

- To select multiple items, hold the SHIFT or CTRL keys (consecutive and nonconsecutive selection).
- When an item is selected, press the space bar to select or clear the check box, which indicates if the item should be included or excluded from the report.

- To select all items at once, check the box in the column header (table view and time line) or check the **Select all** check box (thumbnail view).

Sorting columns

Sort each column alphabetically or by time.

- Click the column header to toggle the order.

Re-ordering the columns

For your convenience, you can change the order of the columns. Your preference is retained for the duration of the session.

- Drag the desired column to the desired location.

Hide or show columns

- Right-click the column header and select the column name in the list.

Viewing more information

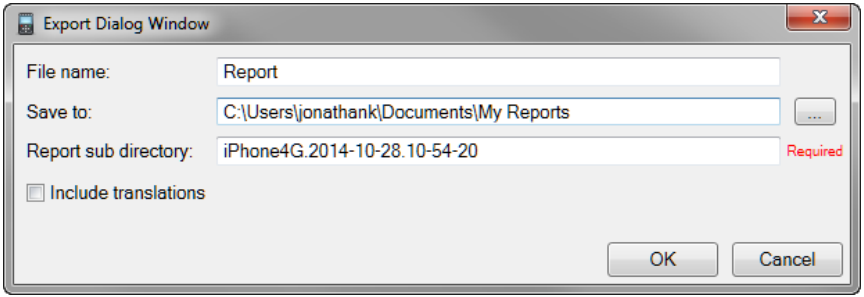
For data tabs containing textual information, by default the right pane is open, displaying the selected item's information.

- To close or open the right pane, click .

Exporting data

1) To export the data in a particular tab, click the desired output in the toolbar: Excel, HTML, PDF, XML, KML (location data only), or EML (email data only).

   The Export Dialog Window appears.



2) Do one of the following:
   - Enter the path where you want to save the report
   - Click ... and browse to and select the desired location.
3) Select the **Include translations** check box to include translated data.
4) Click **OK**.

   The report is generated, and a message appears asking if you would like to open it in third party software.

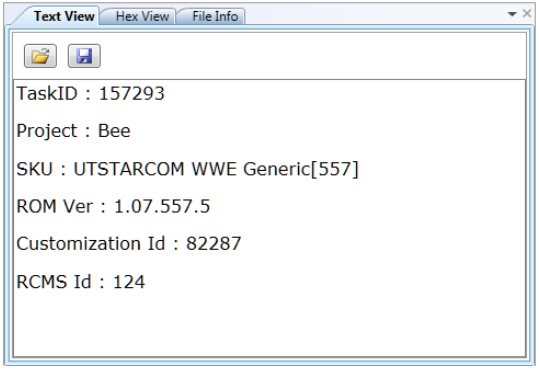
5) Click **Yes** or **No**.

The file is opened in the default third party software.

NOTE: When exporting to EML, a file is created for each email.

4.2.3.2. Text view

For text-based data files, view the data as text.



4.2.3.3. Table view for data files

For data files, the table shows the following information:

	Indicates whether to include (checked) or exclude (unchecked) the item in the report generated.
#	Row number.
	Indicates if the item is bookmarked.
	Indicates whether the data file was deleted , or has an unknown status ("?" or white document icon).
Image	A thumbnail of the image or an icon of the file type. (Image data files only).
Name	The file name.
Path	The root path of the data file.
Size	The size of file.

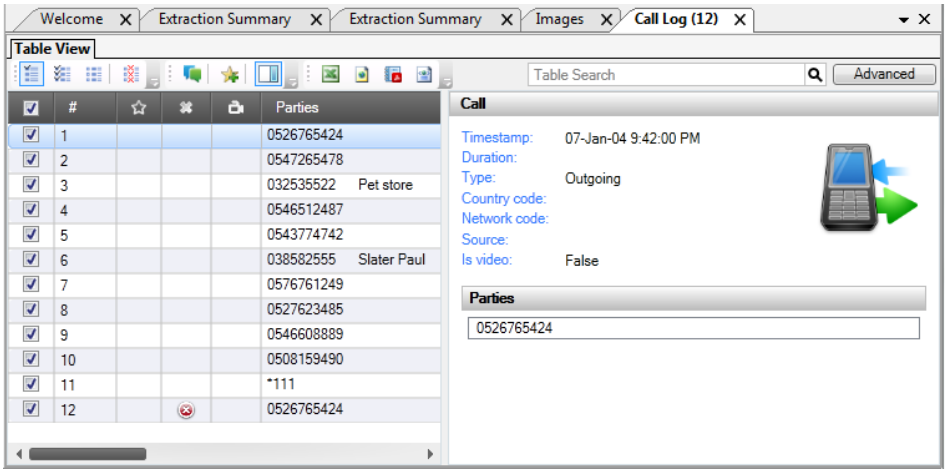
Metadata	Additional metadata of the data file.
Created	The creation time stamp of the data file.
Modified	The modification time stamp of the data file.
Accessed	The last access time stamp of the data file.
Bookmark Note	Details of the bookmark.

In addition, indicators are displayed to show attachments, indicate video calls, and to show even direction.

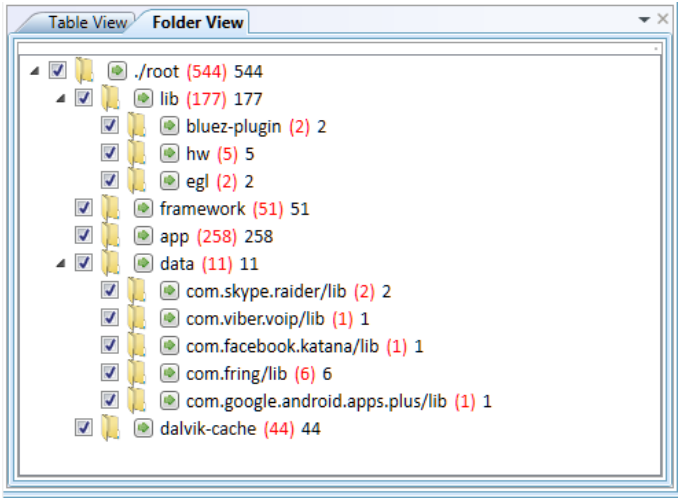
- Double-click on an item record (table row) to open a Hex Viewer tab showing the Hex data of the selected file.

4.2.3.4. Table view for analyzed data

For analyzed data, table view tabs display a list of all the events of a specific type (Call Log, Contacts, SMS messages, and so on) that were found during the data analysis process.



4.2.3.5. Folder view



Folder view shows how the items were organized in the device.

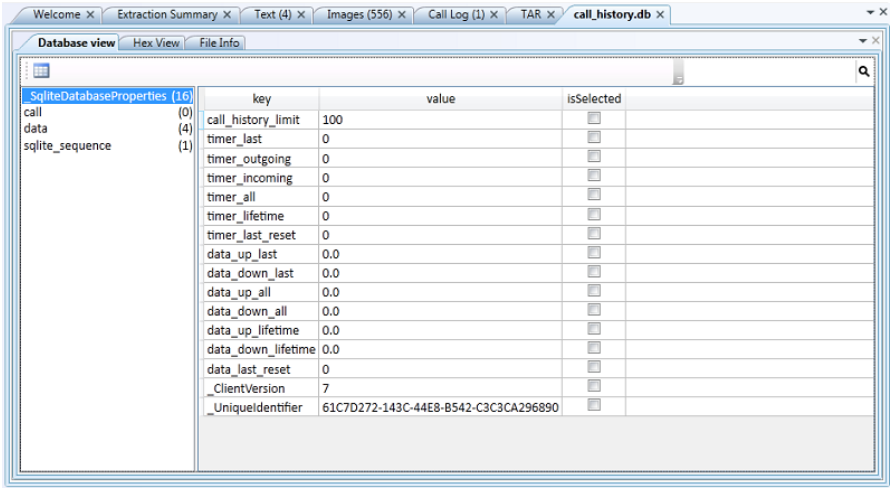
- Select the folder checkbox to select all the items in that folder (including sub-folders). Selected items are included in generated reports. When you select an item, it is selected in all tabs in the data display area.
- Click to open the folder in a new tab in the data display area.

The following folder information is displayed:

- The folder name in the extracted file system.
- The number of selected items in that folder (red in brackets).
- The total number of items in that folder (in black).

4.2.3.6. Database view

- To open database view, open a .db file in the File Systems tree item.



Database view displays the contents of database files that were found in the extraction.

Database view consists of the following sections:

1) List of the database tables.

   A number in parenthesis next to each table name designates the number of records in the database table.

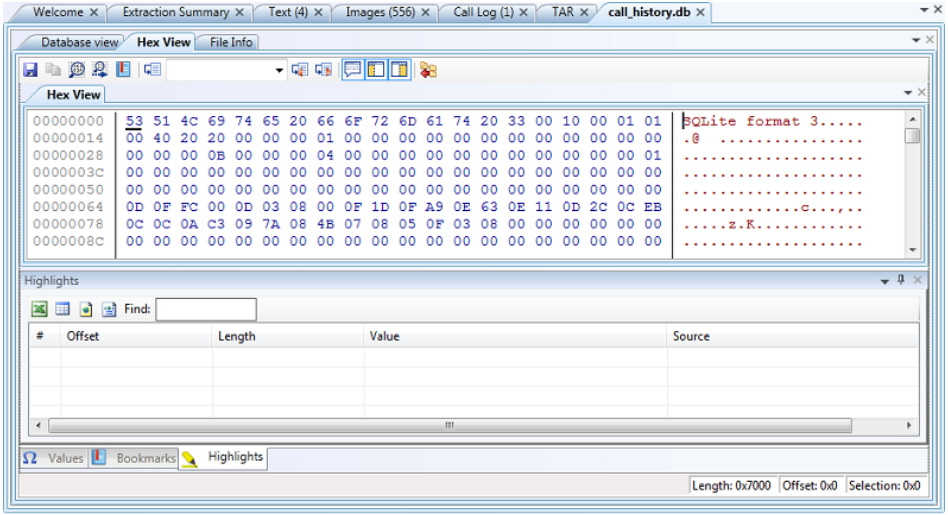
   Select a table in the left column to display its records in the right column.

2) Records display areas containing a list of data records in the selected database table.
3) Search field to filter the displayed records.

- Click to export the selected database records to a CSV file.

4.2.3.7. Hex view

A Hex view tab appears for each binary item you open from the project tree. When opening, for example, an Image memory disk, a Hex view tab opens alone. When opening a binary item, for example, an image file, the Hex view tab may be accompanied by other tabs.



The Hex view tab contains the following sections:

Hex tabs

a) Address column - The number of information column in Hex or Decimal value, displaying the start address of each row in the Hex and ASCII representation data sections

b) Hex data view column - The Hex data of the selected item

c) ASCII representation view column - The ASCII representation of the Hex data

An information frame automatically appears when you position the mouse over the information displayed in the Hex view. The information frame displays links (pointers) to analyzed data items, such as files and folders in the project tree, and search results associated with the pointed data.

Hex view toolbar

	Save	Click to save the entire memory extraction to a local folder.
	Copy Selection	Copy the currently selected content of the Hex View tab to the clipboard.
	Find	Displays the Find dialog to search for all occurrences of specified information in the displayed Hex display pane.
	Find Next	Displays the Find dialog box with the search parameters used in the latest search.
	Add Bookmark	Bookmark the currently selected content of the Hex display pane.
	Go To	Redirect the offset to specific address in the content of the Hex display pane.
	Enable Info Frame	Toggles on/off the display of floating information frame at the cursor location.
	Show Address	Toggles on/off the left address column display.
	Show ASCII view	Toggles on/off the right ASCII representation column display

Analysis information tabs

Located under the Hex view tab are Analysis Information tabs that display the following types of information related directly to the displayed Hex data:

- **Values** - A wide array of value interpretations, such as 8, 16, 32, and 64 bit, various string encoding, date & time formats, and more, calculated on the fly for the currently selected data in the Hex view. See *Working in the Values tab* (page *104*).
- **Bookmarks** - A list of bookmarks added in the displayed Hex data. See *Working with bookmarks* (page *276*).
- **Highlights** - A list of content segments markups highlighted in the displayed Hex data. The number of highlight results is shown in brackets next to the tab name. See *Working in the Highlights tab* (page *106*).
- **Search** - Displays results of a search in the displayed Hex data. A new search results tab opens for each search query performed. The number of results for each search is shown in brackets next to the tab name.

You can rearrange the display of the Analysis Information tabs to suit your preference:

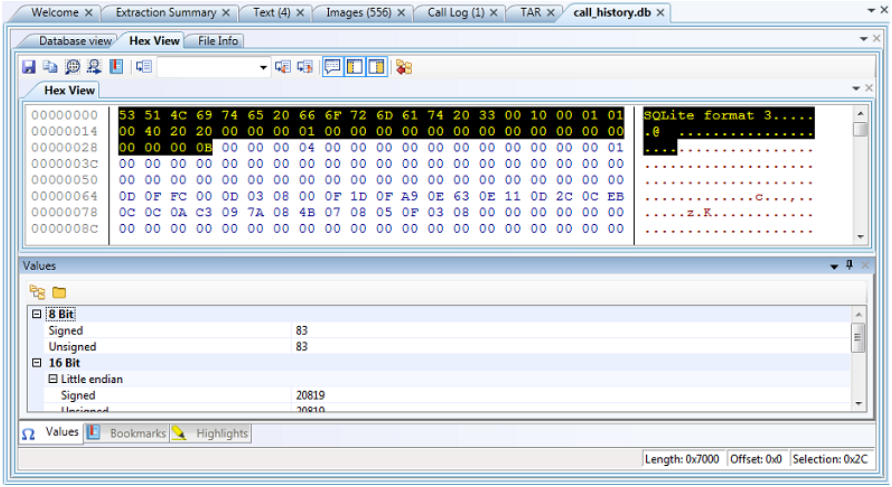
- Double click the header strip of the section to display the entire section as a floating panel. Double click the floating panel header strip to dock it back to the default location (at the bottom of the Hex View tab).

- Double click the name label of any tab to display it as a floating panel. Double click the floating panel header strip to dock it back to the original location.
- Drag the name label or floating panel over any of the docking labels that appear to dock it at that location in the Hex View tab.

4.2.3.7.1. Working in the Values tab

Decode the raw data to a variety of encoding types in real time, and expand them in the Values list.

1) To access the **Values** tab, click the **Values** tab at the bottom of a **Hex view** tab.

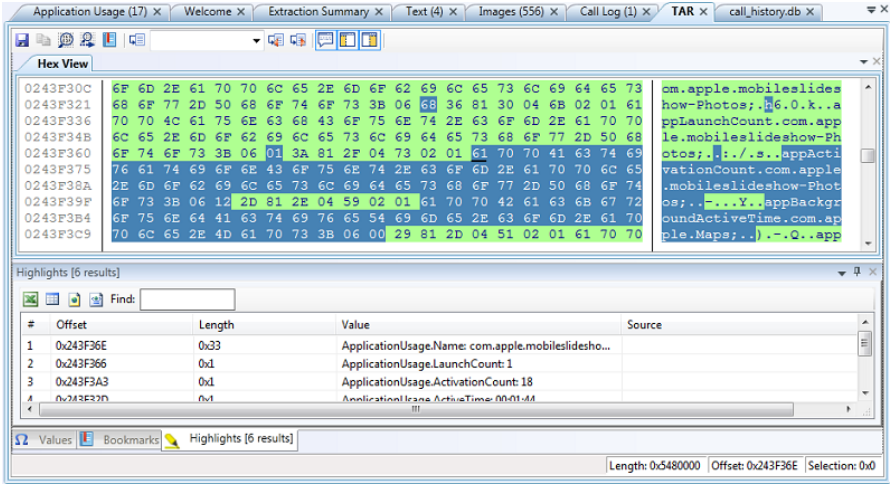


2) Select a data segment in the Hex.
3) To display the decoded data, scroll to the desired encoding, and click ⊞ to expand the display. Some encoding options, such as 16 Bit, have sub-encoding types.
4) Fully expand or collapse all encoding types by clicking or .

4.2.3.7.2. Working in the Highlights tab

The **Highlights** tab contains a list of content segments that are highlighted in the displayed Hex data. Each segment represents locations of analyzed data within the Hex. The **Highlights** tab enables you to locate particular types of analyzed data in the Hex. The number of highlight results is shown in brackets next to the tab name.

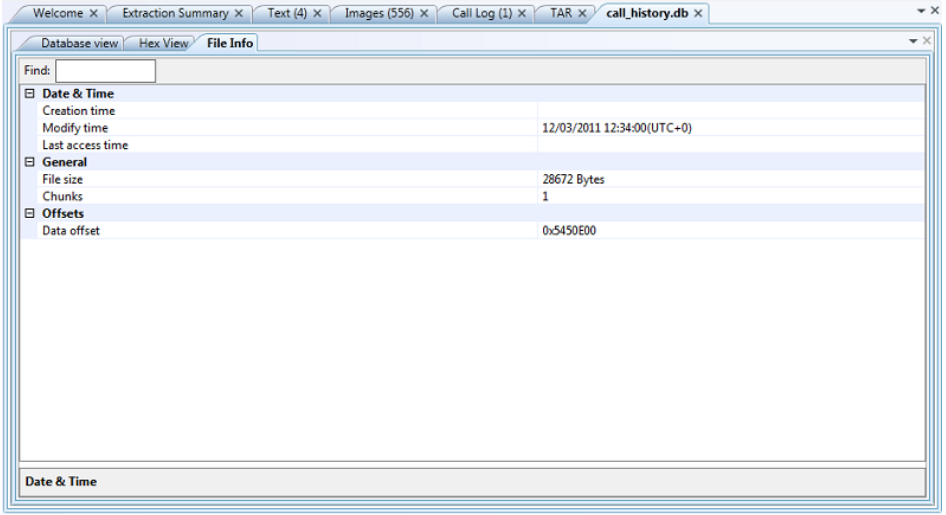
1) To access the **Highlights** tab, click the **Highlights** tab at the bottom of a **Hex view** tab.



2) In the project tree, click an **Analyzed Data** folder (for example, **Contacts**).

The location of the selected folder is highlighted in the **Hex view** tab, and the list of chunks that the folder is comprised of is listed in the **Highlights** tab.

4.2.3.8. File Info tab



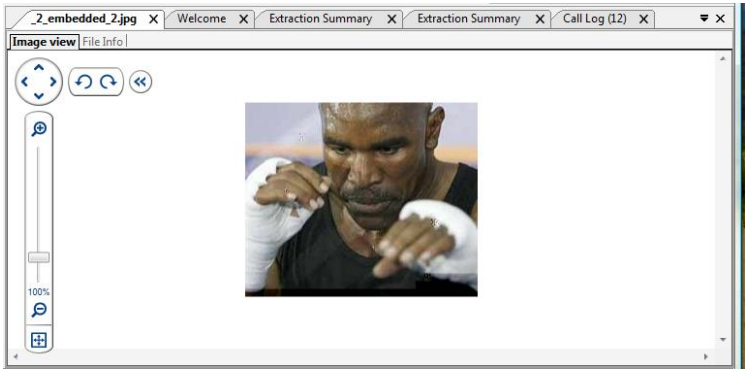
The File Info tab displays the following information about the data file:

- **FAT** – The File Allocation Table of the extended attributes.
- **Date & Time** - Created, Modified, and Last Access time stamps of the data file.
- **General** - The file size in bytes and the number of file system chunks of which the data file is comprised.
- **Offsets** - The offset addresses of the data file in the Hex data.
- **EXIF** - The embedded EXIF information logged by the camera (if it exists).
- **File Metadata** - The general information of the image (capture time, resolution, size and color depth).

4.2.3.9. Viewing image files

1) Double-click an image in a data display tab.

A new tab opens containing the image. The tab is divided into two sub-tabs; **Image view** and **File Info**.



2) In the **Image view** tab, use the image controls:

When the image is enlarged, navigate the image.

Rotate image clockwise and anti-clockwise.

Zoom in and out. You can also adjust the zoom using the slider.

Zoom to fit the tab.

Reset the zoom to 100%.

Hide image controls.

3) Click the **File Info** tab to view the file information. For example, the File metadata section includes information such as the Capture Time, which is the date and time a photo was taken.

4.2.3.10. Playing video files

To play the video within UFED Physical Analyzer:

1) In the data table, double-click the media file that you want to play.

   A new tab opens for the media file.

2) Click .

To play the video in the default program:

- Right-click the media file and select **Open with default program**.

Chapter 5: Locating and analyzing information

This section describes how to browse, search, filter, bookmark, and manage the information in your project.

5.1. Searching for information in a data tab

In **Table View** tabs, search for a particular item within the data table. The search is performed on all the data entries within the table.

- In the **Table Search** box, enter any string.

  The table updates to display only items containing the string you entered.

5.2. Using the quick filter

Use the quick filter tools to filter data in **Table View** tabs as follows:

	Show all	Displays all items
	Only selected	Displays items that are selected
	Only not selected	Displays items that are not selected
	Deleted	Displays deleted items
	Show all	Show all images
	Display images above 30KB	Display only small images above 30KB.
	Display images above 100KB	Display only medium-sized images above 100KB.
	Display images above 500KB	Display only large images (500+KB)
	Filter images (by extension)	Click to enable file type filtering:
	Show JPEG	Display JPG or JPEG files

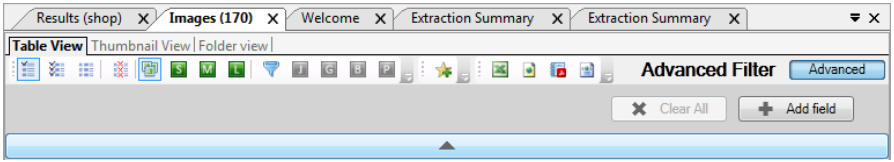
	Show GIF	Display GIF files
	Show BMP	Display BMP files
	Show PNG	Display PNG files
	Metadata filter	Filter image and video files by Metadata (All, Without metadata or Has metadata) and Location (All, Has location or Without location).
	Capture filter time	Filter image and video files by capture time. The maximum range is displayed by default, and you can select a specific date and time range.
	Translation filter	Filter translated text to display all text, translated text or text that has not been translated.

NOTE: The toolbar items are context-sensitive, and only appear when relevant data is displayed.

5.3. Using the advanced filter

Use the advanced filter to filter the list based on a combination of several parameters.

1) In the filter toolbar, click **Advanced**.



2) Click **Add field**, and select a field from the drop-down list. The fields list comprises the columns in the current data tab.
3) In the box that appears for the selected field, enter any string or timestamp.

   The tab displays only items that match the filter.
4) To add additional filters, repeat steps 2-3.

   When you place additional filters in the Advanced search, the returned results match all specified criteria.
5) To clear the string you entered, click .
6) To clear all the entered strings, click **Clear All**.

7) To remove the field filter, click .
8) To close the advanced filter, click **Advanced**.

5.4. Searching for information in all open projects

Use the **All projects** search box in the toolbar to search for information in all open projects.

1) Type any string in the **All Projects** box.

   A list of matching results appear under the **All Projects** search field. The results are sorted by open project. Within each open project, the results are sorted by categories according to type (SMS, messages, contacts, files, and so on). The number of matching results found in each type category is also displayed.

2) Click to collapse or expand the projects.

3) Do one of the following:
   - Click next to the project name to view the results of the search in that extraction in a tab in the data display area.
   - Select **Show All** from the top of the quick results list to display a results tab in the data display area listing all the matching search results. The matching string in each item is colored in red.

   As in the quick results list, the results tab lists the results by type.

5.5. Browsing the file system

UFED Physical Analyzer has the ability to reconstruct and display the device file system in a tree structure.

To browse the device file system:

1) In the **File Systems** tree item, click the ◢ or ▷ icons at every node to expand the tree item.
2) Continue drilling down in the file system to explore its content.

   Files in the reconstructed file system display one of the following icons:

   - - Existing file found in the system
   - - Deleted file data found in the file system
3) When you reach a file that you want to open, double-click it to display its information in the data display area.

The number information tabs displayed for the file changes according to the file type. For example, an unknown file may display only the **Hex View** and **File info** tabs, while a jpeg image may display additional I**mage view** and **Meta data** tabs. The default view is **Hex view**.

For more information on working with Hex view, see *Hex view* (page *100*) and *Working with Hex data* (page *227*)

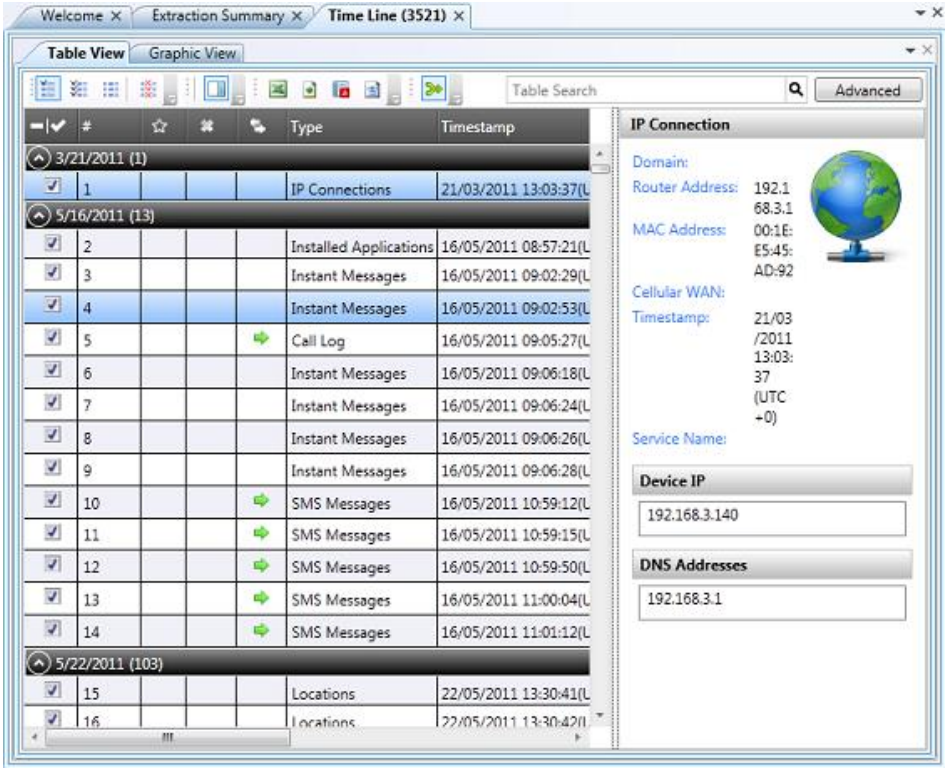
4) While the Hex extraction of an image is displayed in the data display area, click a file under the **File Systems** tree item to highlight the data portion of this file in the Hex data in the data display area.

5.6. Timeline view

Timeline view is a powerful tool that enables you to analyze data in chronological order, to identify the order of events and make connections between them.

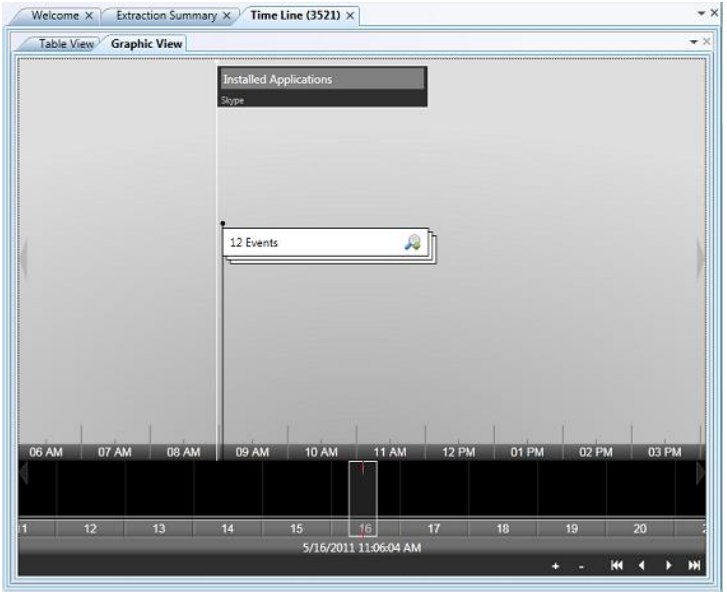
Timeline view has two views; table and graphic.

In table view, the events are displayed in a table, organized by date and time.



- Click to group or ungroup the events by date.

  In graphic view, the events are displayed in a graph, enabling you to quickly identify activity spikes that may be of interest.



- To scroll forwards and backwards in the timeline, use the , , and buttons.

You can increase or decrease the level of detail in the Timeline Graph View:

- To increase the time resolution, click .
- To decrease the time resolution, click .

Events that occur within close proximity are flagged in groups.

- Click to open another timeline view tab for the group of events.

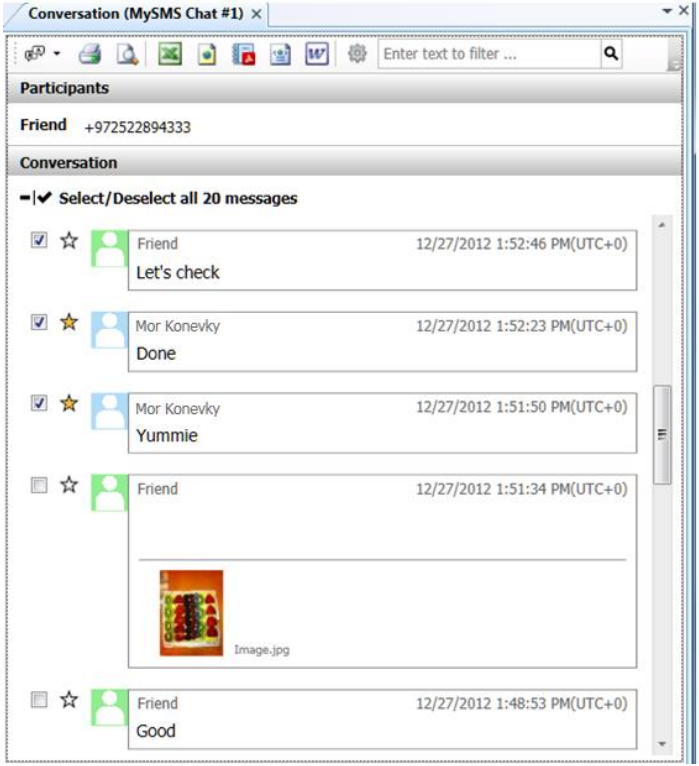
5.7. Accessing conversation view

Communication-based data, such as call logs, email, SMS and MMS messages, and so on, can be displayed in a conversation view layout for easier and better tracking over the communication between two or more parties. You can search for messages within a chat, select the messages to include within a report (by default all chat messages are included), print, or export the conversation.

To access and use conversation view:

1) In a communication-based data table, select one of the records.
2) Click .

   A conversation tab opens, displaying related items as a conversation between the sending and receiving parties of the selected item.


Conversation (MySMS Chat #1)
Enter text to filter ...
Participants
Friend +972522894333
Conversation
Select/Deselect all 20 messages
Friend 12/27/2012 1:52:46 PM(UTC+0)
Let's check
Mor Konevky 12/27/2012 1:52:23 PM(UTC+0)
Done
Mor Konevky 12/27/2012 1:51:50 PM(UTC+0)
Yummie
Friend 12/27/2012 1:51:34 PM(UTC+0)
Image.jpg
Friend 12/27/2012 1:48:53 PM(UTC+0)
Good

3) To translate or delete translated text, click and then select **Translate all** or **Delete all translations**.
4) To print the conversation, click .
5) To view a print preview, click .
6) To export the conversation, click the desired output in the conversation tab toolbar: Excel , HTML , PDF , XML , or Word .
7) To change the order of the conversation, click and then select **Oldest message first**, or **Newest message first**.
8) To filter messages, enter text in the search box.
9) To add or edit bookmarks, click .
10) Select a check box to include specific messages in the report, (or select all messages or no messages).

5.8. Working with watch lists

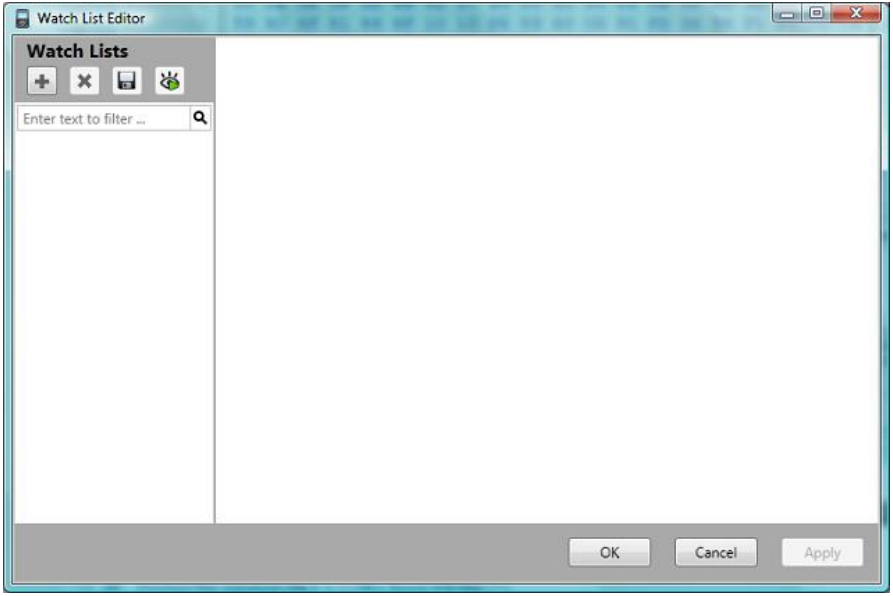
Run a watch list of keywords against your extracted data to identify and highlight important and relevant information.

The watch list search can either be activated automatically or run manually on selected decoded data.

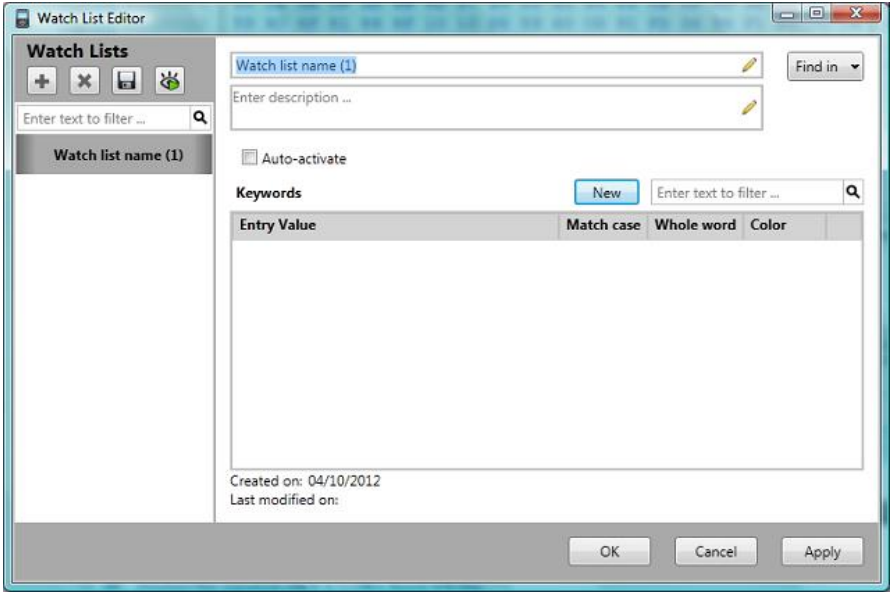
5.8.1. Creating a watch list

1) Do one of the following:
    - In the toolbar, click .
    - In the **Tools** menu, select **Watch List Editor**.

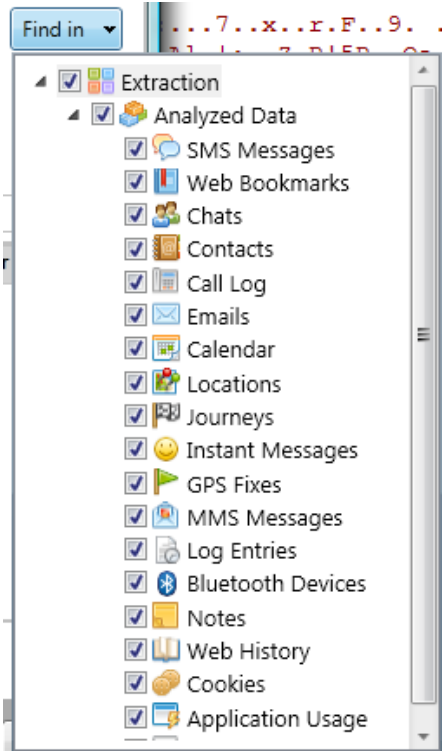
The Watch List Editor appears.



2) Click , and select **New**.



3) In the **Watch list name** box, enter a name for the watch list.
4) To set the watch list to find keywords only in data types in the project, click **Find in**, and select the desired data types.



When you run the watch list, only selected data types are checked for matches.

5) In the **Enter description** box, enter a general description for the watch list (optional).
6) To set the watch list to run automatically when you open projects, click **Auto-activate**.
7) Click **New** to add a new keyword.

   A new keyword row appears in the Keywords list.
8) For each keyword, set the following, as desired:
   - **Entry Value**: Enter the keyword.
   - **Match case**: Select to match the case of the keyword
   - **Whole word**: Select to match the whole keyword.
   - **Color**: Click and select the color you want matched keywords to be shown in.
9) Do one of the following:
   - Click **Apply** to save the watch list and keep the Watch List Editor open.
   - Click **OK** to save the watch list and close the Watch List Editor.
   - Click **Cancel** to close the Watch List Editor without saving your changes.

5.8.2. Editing a watch list

1) In the Watch List Editor, select the watch list that you want to edit.
2) Edit the watch list parameters and keywords that you want to change.
3) To filter the keyword list to locate a particular keyword, type the keyword in the **Enter text to filter** box.
4) To edit a keyword, click the relevant keyword in the list, and make the desired changes.

5) To delete a keyword, click .
6) When you have finished making changes, do one of the following:
    - Click **Apply** to save the watch list and keep the Watch List Editor open.
    - Click **OK** to save the watch list and close the Watch List Editor.
    - Click **Cancel** to close the Watch List Editor without saving your changes.

5.8.3. Importing a watch list

The export and import functions enable you to share watch lists and receive watch lists from your colleagues. Import existing watch lists (*.csv files) that were saved from or created by UFED Physical Analyzer.

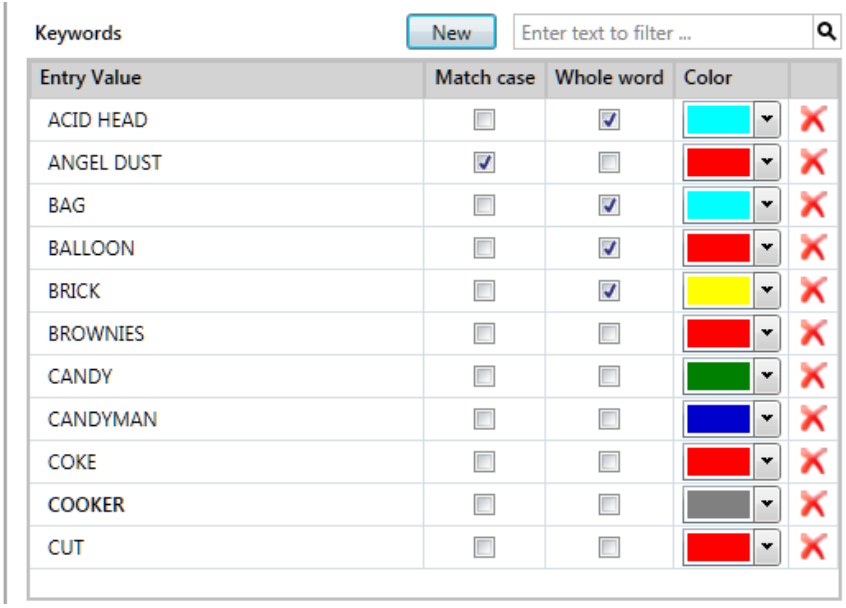
You can also import a CSV file that contains a list of keywords, which can then be used as watch list keywords. This option will import the keywords without any formatting and will look to find all data types by default.

1) In the main toolbar, click .

    The Watch List Editor appears.

2) Click , and select **Import**.
3) Browse to the location where your watch list is saved, select the CSV file, and click **Open**.

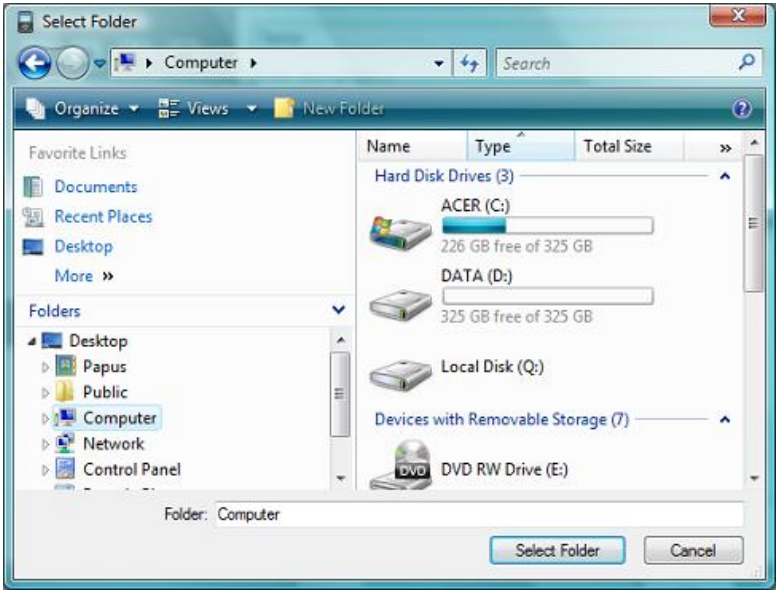
    The watch list appears in the Watch List Editor. An example is displayed next.


Keywords
New
Enter text to filter ...
Entry Value
Match case
Whole word
Color
ACID HEAD
ANGEL DUST
BAG
BALLOON
BRICK
BROWNIES
CANDY
CANDYMAN
COKE
COOKER
CUT

5.8.4. Exporting a watch list

Export watch lists to save the watch list as a *.csv file for later use, or to share with others.

1) In the Watch List Editor, select the watch list that you want to export.
2) Click .

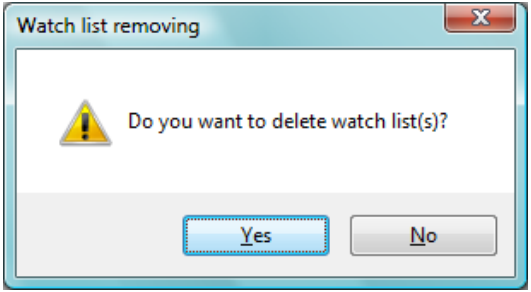


3) Browse to the location where you want to save your watch list, and click **Select Folder**.

   The watch list is exported. It will be saved by default as [name of watch list].csv.

5.8.5. Deleting a watch list

1) In the Watch List Editor, select the watch list that you want to delete.
2) Click .



3) Click **Yes**.

   The watch list is deleted.

5.8.6. Running a watch list

You can run watch lists on open projects.

5.8.6.1. Running a watch list on particular projects

When you run a watch list from the Watch List Editor, you can select which watch lists to run, and on which projects you want to run them.

1) In the toolbar, click to open the Watch List Editor, and select the watch list you want to run.
2) Click .

   A list of open projects appears.
3) Select the open project(s) that you want to run the search on.

   NOTE: A tick mark shows that the selected watch list is currently active for the project.
4) Click **Apply**.

   UFED Physical Analyzer searches for keywords in the selected project(s). When complete, the watch list results appear in the **Watch Lists** tree item.

   If the watch list is assigned to only particular information types (see *Creating a watch list* (page *123*)), only matches to those types appear in the watch list results.

5.8.6.2. Running a watch list on your current project

When you run a watch list from the project tree, you can select which watch lists to run on the project that you are currently working in. If you have more than one project open, the selected watch lists run on the project that you last clicked in in the project tree.

1) In the toolbar, click .

   A list of watch lists appears.

2) Select the watch list(s) that you want to run on the project you are currently working in.

   NOTE: A tick mark shows that the watch list is currently active for the project.

3) Click **Apply** on the project that is in focus in the project tree.

   NOTE: When you click from the toolbar, you can only run the watch list(s) on the project that you last clicked in in the project tree.

   UFED Physical Analyzer searches for keywords in the selected project(s). When complete, the watch list results appear in the **Watch Lists** tree item.

   If the watch list is assigned to only particular information types (see *Creating a watch list* (page *123*)), only matches to those types appear in the watch list results.

5.8.7. Locating a watch list

1) Do one of the following:
    - In the toolbar, click .
    - In the **Tools** menu, select **Watch List Editor**.

   The Watch List Editor appears.
2) In the **Enter text to filter** box, enter the watch list name in whole or in part and click .
3) The list of watch lists is filtered accordingly.

5.9. Bookmarking information (entity bookmarks)

An entity bookmark is a quick reference pointer you can create on individual items:

- An **Analyzed Data** item such as a call from the call log, a contact record, an email message, etc. See the *Analyzed Data* item in *Project tree* (page *70*).
- A **Data Files** item such as an image file, a video file, a text file, and so on. See the *Data files* item in *Project tree* (page *70*).

The entity bookmarks you create are managed in the **Entity Bookmarks** tree item. The number of entity bookmarks in the project is shown in brackets next to the section name.

- Double-click **Entity Bookmarks** to list the entity bookmarks in a tab in the data display area. Selected entity bookmarks are included in reports that you generate.

- Double-click any entity bookmark to go to the bookmarked item in the appropriate display tab.

  For example, double-click an entity bookmark to an SMS message to open the list of SMS messages in an Analyzed Data display tab, with the bookmarked item highlighted.

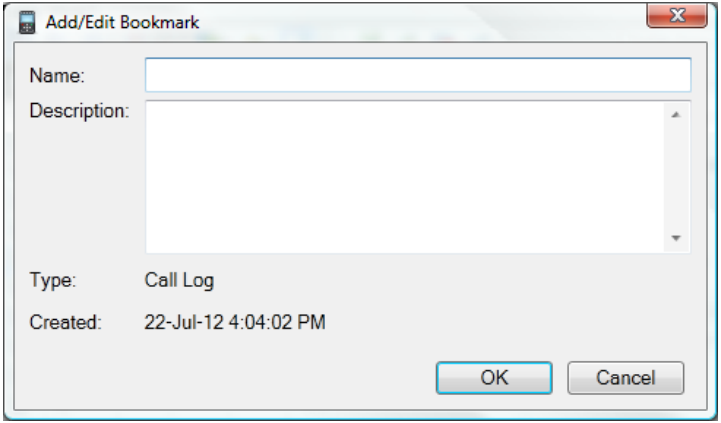
- Hover over a to display the bookmark name and description.
- To print or export just the entity bookmarks list, click the desired output in the **Entity Bookmarks** tab toolbar: Excel , HTML , PDF , or XML .

5.9.1. Creating a new entity bookmark

Entity bookmarks can be added to items in Table view.

1) Select the item you want to bookmark.
2) Click .

The Add/Edit Bookmark dialog box appears.



3) Enter a name and a description to the new entity bookmark, then click **OK**.

   A new entity bookmark pointing to the selected item is added to the entity bookmarks list of the project. The bookmarked item record is marked with a ★.

5.9.2. Editing an entity bookmark

1) Select one of the following:
   - An entity bookmark record from the list of **Entity Bookmarks** in the project tree.
   - A bookmarked item (marked with ★).

2) Click in the Table view toolbar.

   The Add/Edit Bookmark dialog box appears.

3) Edit the name or description, then click **OK**.

5.9.3. Deleting an entity bookmark

1) Select one of the following:
   - An entity bookmark record from the list of **Entity Bookmarks** in the project tree.
   - A bookmarked item (marked with).
2) Click in the Table view toolbar.

   The bookmark is deleted.

5.10. Device Locations

5.10.1. About location data

In UFED Physical Analyzer, location data is drawn from different locations within the device. The following location data is analyzed:

Analyzed data > Locations

Location data in the **Locations** item is divided into the following categories:

- Cell towers
- WiFi networks
- Harvested Cell towers
- Harvested WiFi networks
- Media locations

Harvested and non-harvested location information

Harvested and non-harvested location information is taken from the device database.

The device location is identified by the device's GPS information, which is calculated in two ways:

1) Collection - As the device changes locations when traveling with its owner, it collects the location information of each cell tower and Wi-Fi Network Receptor as it enters their vicinity. These locations are called "harvested" information. The location calculated in this way is considered accurate.

   When the device Wi-Fi is turned on, the device periodically sends the harvested locations to Apple (iPhone devices) or Google (Android devices). The harvested information is then deleted from the device.

When the device Wi-Fi is turned off, or there is no Wi-Fi connection available, the device harvests and stores the locations of the cell towers and Wi-Fi networks, and then sends the information when the Wi-Fi is turned on, or connection is available.

2) Download - The device connects to the location services provider (Apple (iPhone devices) or Google (Android devices), requesting location services. Apple or Google send information about cell tower and Wi-Fi networks in a ~2km radius. This information is saved on the device and is called "non-harvested" information.

Location data in the Cell towers, WiFi networks, Harvested Cell towers, and Harvested WiFi networks categories includes:

- GPS information - longitude and latitude
- Accuracy - radius in meters within which the device is located.
- Confidence - in %. How confident the service provider is that the phone indeed lies in the calculated location.
- Timestamp

Media locations

Location data in **Media locations** is taken from the location stamp associated with each media file.

Analyzed data > Journeys

Location data in the **Journeys** item is taken from the GPS applications on the device. The categories displayed in this item are divided by application.

Analyzed data > GPS fixes

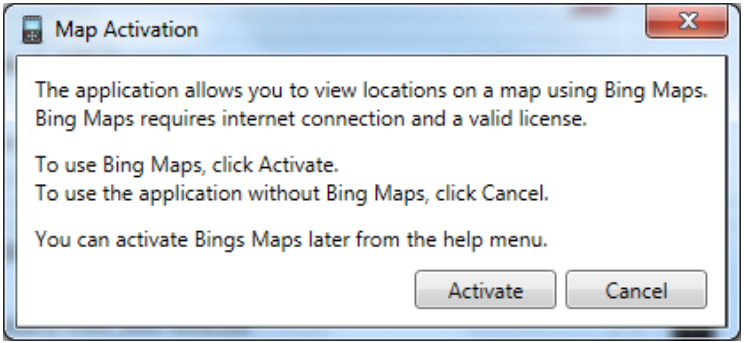
Location data in the **GPS fixes** item is taken from GPS devices and GPS applications on the device. The categories displayed in this item are divided by application and source.

5.10.2. Viewing location data on BING

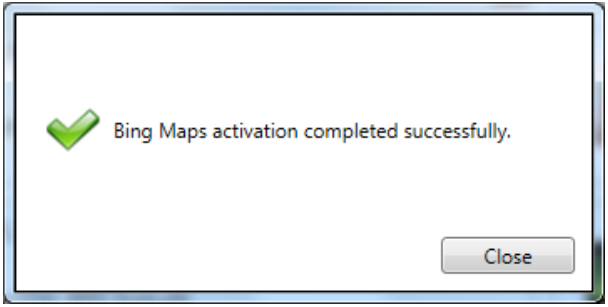
The maps function is free of charge but requires internet access. It is only available to UFED Physical Analyzer users with a valid license.

To activate Bing maps:

The first time UFED Physical Analyzer is started you will be asked to activate your Bing maps. The following screen is presented:


Map Activation
The application allows you to view locations on a map using Bing Maps.
Bing Maps requires internet connection and a valid license.
To use Bing Maps, click Activate.
To use the application without Bing Maps, click Cancel.
You can activate Bings Maps later from the help menu.
Activate
Cancel

- Click **Activate** to activate your Bing maps. After activation the following screen is presented:



If activation is not performed at startup, Bing maps can be activated later via the **Help** menu.

Users can browse and search topographically-shaded street maps for many cities worldwide. Two primary types of street map views are available to users: Road View, Aerial View

Road View

Road view is the default map view and displays vector imagery of roads, buildings, and geography.

Aerial View

Aerial view overlays satellite imagery onto the map and highlights roads and major landmarks for easy identification amongst the satellite images.

5.10.3. Markers and information windows

Markers signify the location where a person's device registered.

The color of the marker signifies which person was registered at a particular location. At a low zoom level, markers show the approximate location, and may include the data of more than one person.

The following markers are examples of the types of markers that are displayed in the map:

At low zoom level, this marker displays a number of recorded locations in a particular area.

Indicates the location of the cell tower that registered the person's device.

Indicates the location of the WiFi network receptor that registered the person's device.

Indicates the recorded location or a media object.

Indicates the location of an unidentified entity that registered the person's device.

5.10.4. Retrieving addresses

You can view street addresses for longitude and latitude positions extracted from a device. This can then be used to filter the locations. You can select single or multiple locations up to a maximum of 200. You can retrieve street addresses in the following views: Project search, Timeline views and Watch List results.

NOTE: To use this feature, you must activate the Bing map service and be connected to the Internet.

To retrieve an address:

1) In one of the Device locations table views, select a row, right-click and select **Retrieve address**, or click .

   NOTE: To retrieve multiple addresses, you can use Ctrl button to select the locations.

	Timestamp	Position	Map Address
	1/25/2011 3:29:27 PM(UTC+0)	(46.244610, -70.801400)	Beauceville, QC, Canada
	1/25/2011 2:29:00 PM(UTC+0)	(46.779900, -71.267570)	
	1/25/2011 1:20:30 PM(UTC+0)	(46.788060, -71.281680)	787 Avenue Nérée-Tremblay, Quebec, QC G1V 4K3, Canada
	1/25/2011 12:19:45 PM(UTC+0)	(46.788470, -71.282010)	
	1/25/2011 11:16:02 AM(UTC+0)	(46.803410, -71.231840)	330 Rue Père-Marquette, Québec, QC G1S 1Y8, Canada
	1/25/2011 10:15:08 AM(UTC+0)	(46.778810, -71.261080)	2186 Rue Brulart, Quebec, QC G1T 1G4, Canada

   The retrieved addresses are displayed in red in the column called Map Address.

To filter locations:

- Click and then select one of the following options:
    - **Show All** to display all locations.
    - **With map address** to display locations that have a map address.
    - **Without map address** to display locations that do not have a map address.

Chapter 6: **Translating decoded data**

Translate the content in your extractions that are in foreign languages without having to wait for a translator to become available, or to use Internet-based tools.

The Translation feature enables you to translate decoded data on demand, so that an investigator can understand the information available in an extraction. The Translation feature is an offline translation solution, where you do not need to be connected to the Internet. You can select single, multiple or all table entries for translation. Both the original and the translated text can be included in the report.

The lists of supported languages are as follows:

Chinese (Simplified)
Chinese (Traditional)
Dutch
German
Hebrew
Italian
French
Japanese (requires additional payment)
Korean
Polish
Portuguese
Russian
Spanish
Ukrainian

6.1. Using the feature

To use this feature, you need do the following:

- Update your license with the selected languages
- Download the translation pack
- Translate the decoded data

6.2. Updating your license with the selected languages

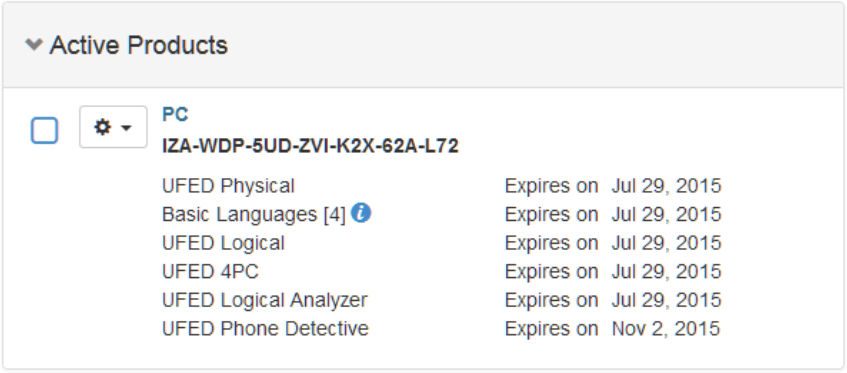
You can select up to five languages for free from the My Products page in MyCellebrite. If additional languages are required, you can purchase the Basic Language Package. You cannot change a language after saving, but you can request additional languages.

NOTE: If you want to translate to a language other than English, you should select it as well.

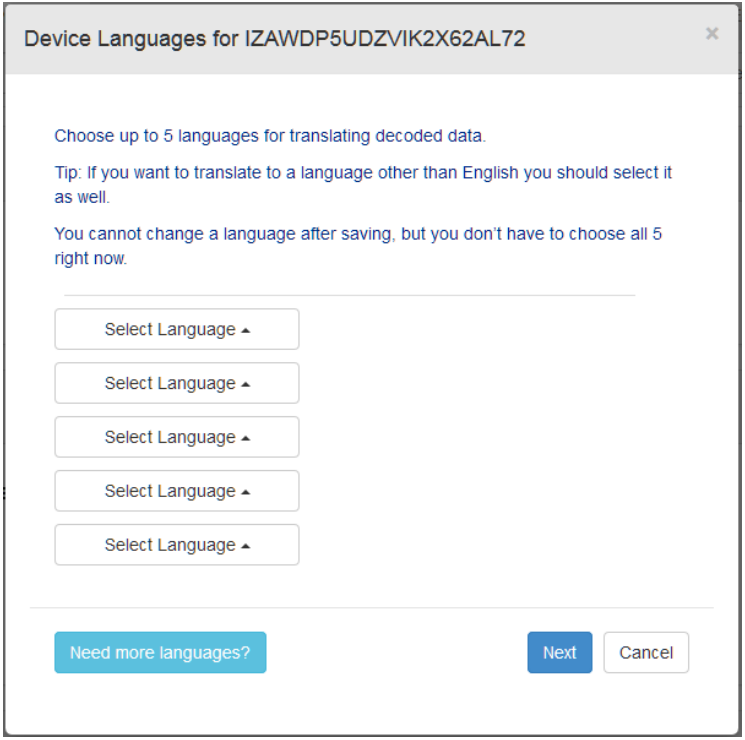
6.2.1. Selecting languages in MyCellebrite

To select languages:

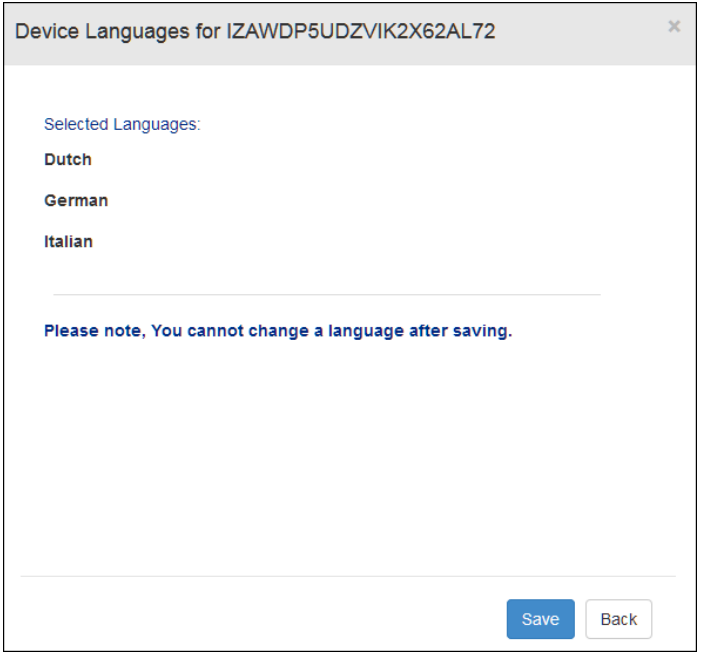
1) Log in to MyCellebrite and select the **My Products** tab. The following window appears.



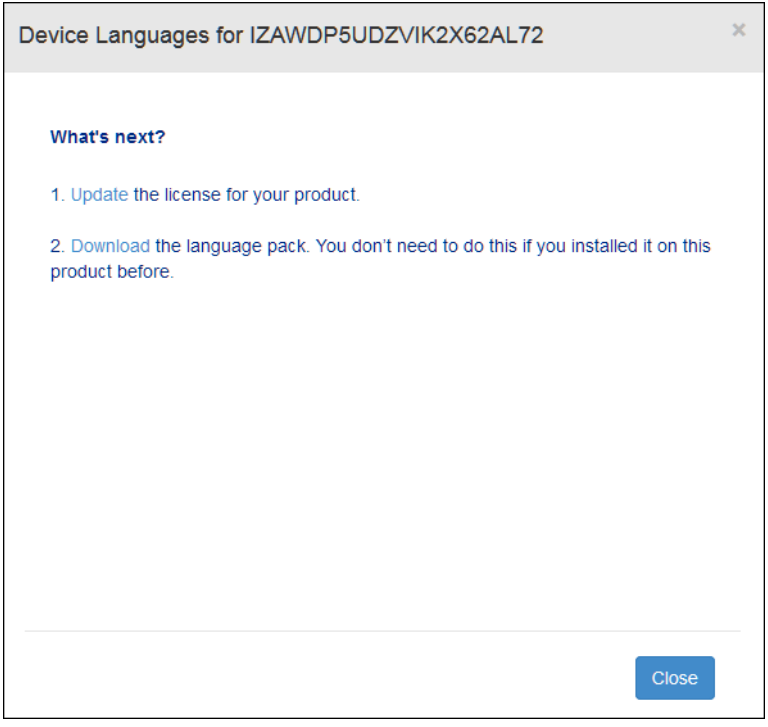
2) Select and click **Select Languages**. The following window appears.


Device Languages for IZAWDP5UDZVIK2X62AL72
Choose up to 5 languages for translating decoded data.
Tip: If you want to translate to a language other than English you should select it as well.
You cannot change a language after saving, but you don't have to choose all 5 right now.
Select Language
Select Language
Select Language
Select Language
Select Language
Need more languages?
Next
Cancel

3) Select up to five translation languages and click **Next**. The following window appears. For additional languages, click **Need more languages** and complete the form.



4) Click **Save**. The following window appears.


Device Languages for IZAWDP5UDZVIK2X62AL72
What's next?
1. Update the license for your product.
2. Download the language pack. You don't need to do this if you installed it on this product before.
Close

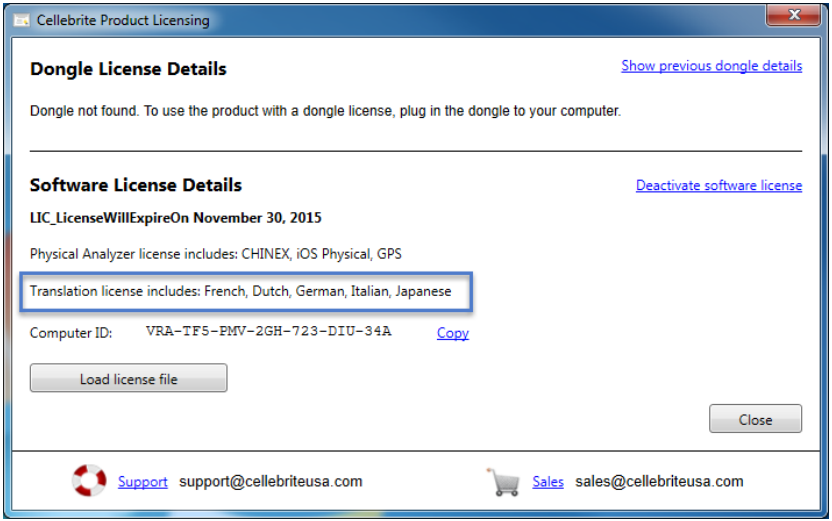
5) Update the license for the product and download the language package.

After updating your product license with the selected languages, you can use the following procedure to view the languages included in the translation license.

To view the translation license languages:

- Select **Tools** > **Translation** > **Show supported languages**.

  The following screen appears.


Cellebrite Product Licensing
Dongle License Details
Show previous dongle details
Dongle not found. To use the product with a dongle license, plug in the dongle to your computer.
Software License Details
Deactivate software license
LIC_LicenseWillExpireOn November 30, 2015
Physical Analyzer license includes: CHINEX, iOS Physical, GPS
Translation license includes: French, Dutch, German, Italian, Japanese
Computer ID: VRA-TF5-PMV-2GH-723-DIU-34A
Copy
Load license file
Close
Support support@cellebriteusa.com
Sales sales@cellebriteusa.com

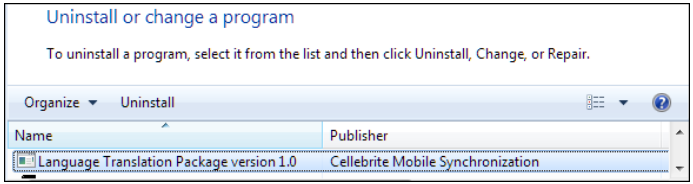
6.2.2. Downloading the translation pack

You can download the Translation pack from the application or from your my.cellebrite.com account. The Translation pack includes a version number, which enables you to track the version installed on the computer.

To download the translation pack:

1) Select **Tools** > **Translation**.
2) Select one of the following options:
    - **Download translation pack:** Downloads the translation pack (this option is not available if there is no Internet connection).
    - **Install translation pack from file:** Installs the translation pack from a file. Select this option if there is no Internet connection.
3) Follow the on-screen instructions to install the Translation pack.

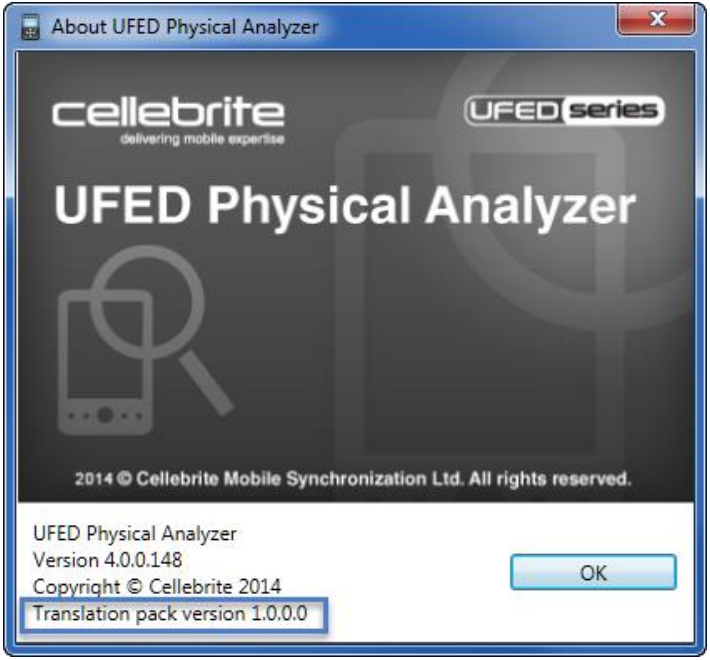
NOTE: To uninstall the Translation pack, go to the Windows Uninstall page, and select the Language Translation Package, (Publisher: Cellebrite Mobile Synchronization) from the list.


Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Uninstall
Name
Publisher
Language Translation Package version 1.0
Cellebrite Mobile Synchronization

To view the translation pack version number:

- Click **Help** > **About**.

  The following screen appears.



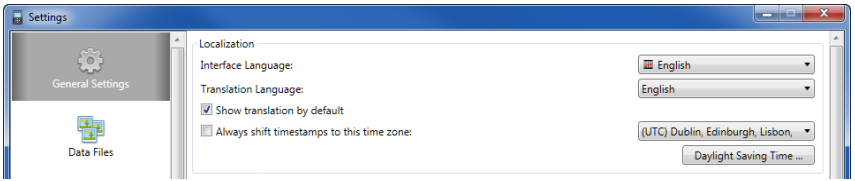
6.2.3. Translating the decoded data

By default, the target language is set to the same language as the interface language. If required, you change the target language to a different language.

To change the translation language:

1) Select **Tools** > **Settings**.

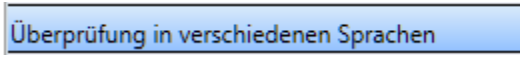
   The following screen appears.



2) Select the Translation Language. That is the language to which you want to translate the text. You can only select one Translation Language. To request additional translation languages, select **Get more languages**.
3) Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text. To see the translation select **View translated**.

To translate decoded data:

1) Click to select the data that you want to translate.

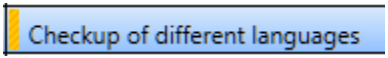


2) Click the button, or right-click and select **Translate selected** or click and then select one of the following options:

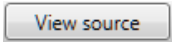
- **Translate all:** Translate all entries in the specified view.
- **Translate selected:** Translate the select text only.

NOTE: If required, use the **Delete translation** option to delete the translated text.

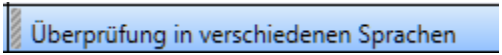
The translated text is indicated by a yellow bar.



To view the original text:

1) Right-click the text and select **View source**, or click the  button.

The original text is indicated by with a gray bar.



To filter text:

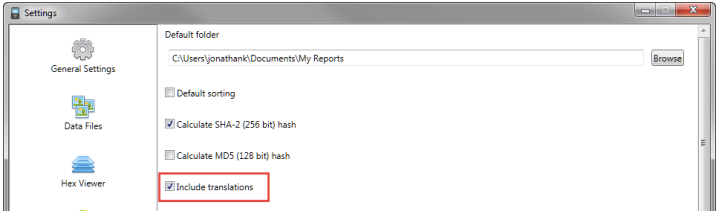
- Click and then select one of the following options:
    - **All** to display all text.
    - **Translated** to display text that has been translated.
    - **Not translated** to display text that has not been translated.

6.2.4. Reporting

When creating reports or exporting data, you can specify whether to include the translated text or not. If you choose to display the translated text within the report, the summary table will include an additional entry called: Translated languages, with a list of the languages. The translated content appears below the original text under the heading: Translation. For more information on reports, see Generating a report on page *173*.

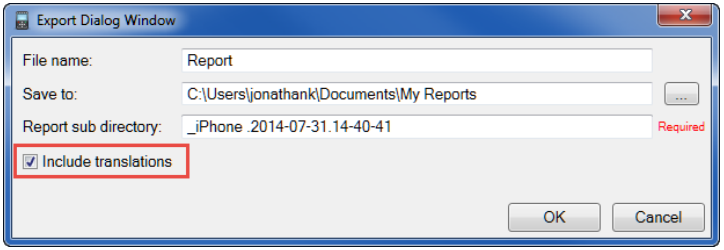
To include the translated text in reports:

1) Go to **Tools** > **Settings** > **General Settings** > **Report Defaults**.
2) Select the **Include translation** check box.



To include translated text in exports:

1) Click an Export option ( ).
2) Select the **Include translation** check box.



Chapter 7: **Working with project analytics**

Project Analytics enables you to view the extraction data in terms of the number of communication events between the device and other parties, identified by phone number, or other user identity (such as email address, Skype handle, and so on). The analysis enables you to easily and efficiently identify communication patterns between the device and other parties. For example:

- Parties most communicated with via all types of communication methods
- Parties most communicated with via phone calls, SMS, and MMS

If the device user exchanged a large number of phone calls, SMS, and emails with a certain contact, it is easy to see the volume of this communication.

Communication events are listed by volume per type. The following communication events are supported:

- **Phones** - Lists outgoing, incoming, and missed calls, and sent, received, and draft SMS and MMS.
- **Emails** - Lists emails sent, received, drafts, and emails of unknown status.
- **WhatsApp -** Lists messages sent, received, and drafts.
- **Skype -** Lists calls, SMS, and chat messages.
- **BlackBerry Messenger -** Lists chat messages.

Project analytics runs automatically when you open an extraction file.

To view project analytics:

1) Click ⊞ next to the **Project Analytics** tree item to view the analytics results displayed in the **Project Analytics** tree item.
2) Double-click the **Project Analytics** tree item to open a tab that displays the top five activities per contact.
3) To view a comparative overview of all communication events, double-click the **Activity Analytics** tree item. The view is sorted in descending order, based on the total number of events.

4) To view the events by communication identifier, double-click the desired identifier tree item.
5) Click the column header to sort the information in the column.

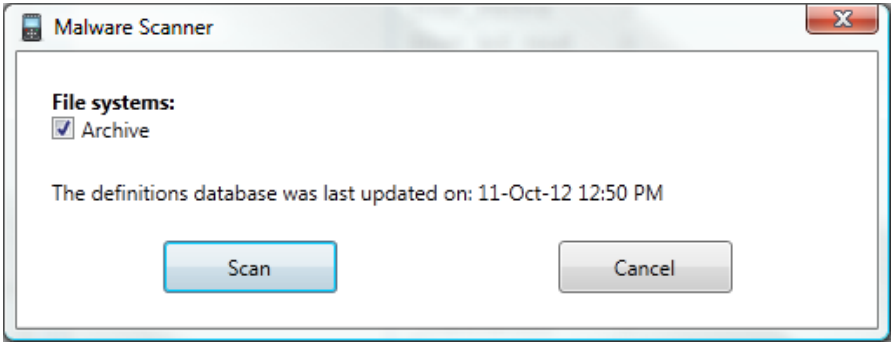
NOTE: Project analysis information can be included in a report. For more information, see Generating a report.

Chapter 8: **Scanning for malware**

Run malware detection on your extraction to search for malware.

When you scan for malware, UFED Physical Analyzer uses the last-used signature database. If this is the first time you are using the malware scanner, or if you want to update the database before you scan, follow the steps in *Updating the signature database (online)* (page *164*). If you are working on a computer without an internet connection, follow the steps in *Updating the signature database from file (offline)* (page *166*).

1) Select **Tools** > **Malware Scanner** > **Scan Malware** or click .



2) Select the file system(s) that you want to scan, and click **Scan**.

UFED Physical Analyzer scans the project for malware. The results are displayed under the **Malware Scanner** tree item.

3) Double-click the **Malware Scanner** tree item to open a data display tab.

   The data shown includes the malware type and malware information, such as the name.

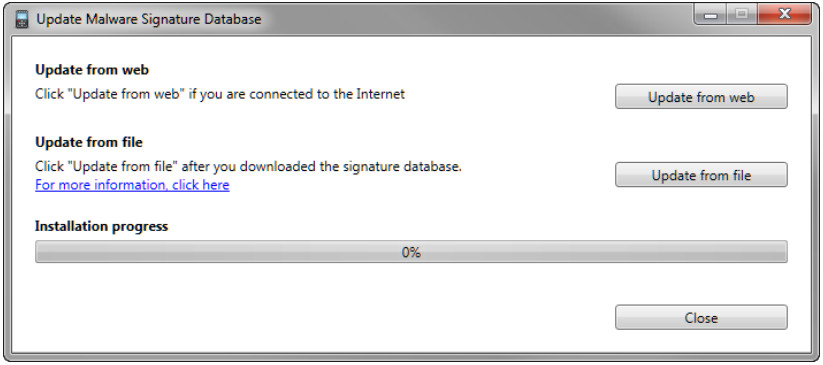
- To include the results in a report, select **Infected Files** in the **Report Dataset** area. For more information, see *Generating a report*.

8.1. Updating the signature database (online)

Update the signature database before the first time you use the malware scanner in order to populate the database, and thereafter in order to keep the signature database up to date.

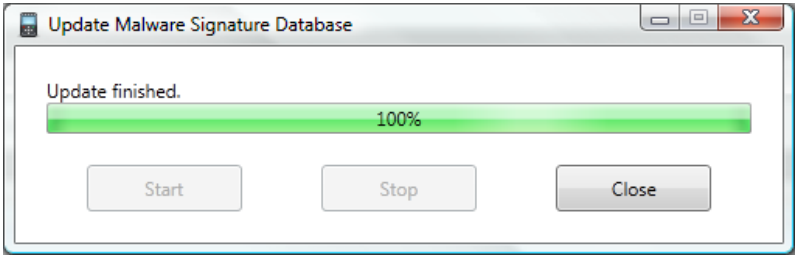
NOTE: Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

1) In the **Tools** menu, select **Malware Scanner** > **Update signature database**.


Update Malware Signature Database
Update from web
Click "Update from web" if you are connected to the Internet
Update from web
Update from file
Click "Update from file" after you downloaded the signature database.
For more information, click here
Update from file
Installation progress
0%
Close

2) Click **Update from server**.

The database is populated.



3) Click **Close**.

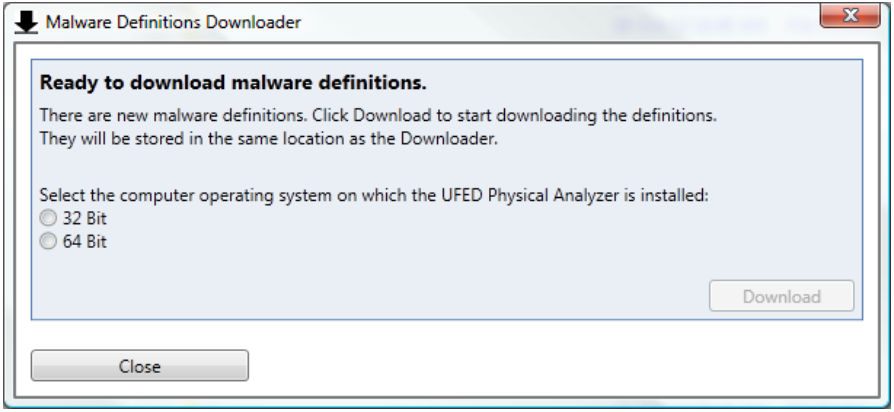
You can now scan the project for malware.

8.2. Updating the signature database from file (offline)

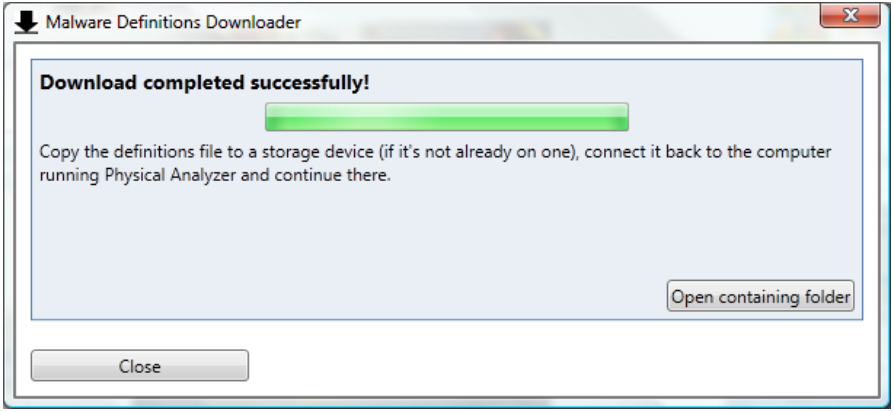
Update the signature database from file when you are working on a computer that does not have an internet connection.

NOTE: Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

1) In Windows Explorer, in the main UFED Physical Analyzer directory, copy the **BitDefenderUpdater** directory to an external storage device.
2) Transfer the **BitDefenderUpdater** directory to a computer that has internet connection without proxy settings.
3) In the **BitDefenderUpdater** directory, double-click **Malware Definitions Downloader.exe**.


Malware Definitions Downloader
Ready to download malware definitions.
There are new malware definitions. Click Download to start downloading the definitions.
They will be stored in the same location as the Downloader.
Select the computer operating system on which the UFED Physical Analyzer is installed:
32 Bit
64 Bit
Download
Close

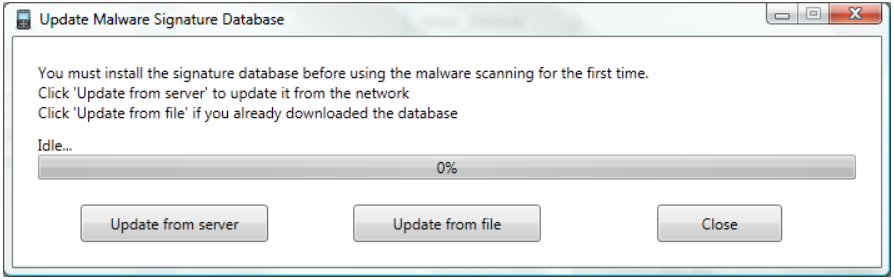
4) Select the computer operating system of the computer on which UFED Physical Analyzer is installed.
5) Click **Download**.


Malware Definitions Downloader
Download completed successfully!
Copy the definitions file to a storage device (if it's not already on one), connect it back to the computer running Physical Analyzer and continue there.
Open containing folder
Close

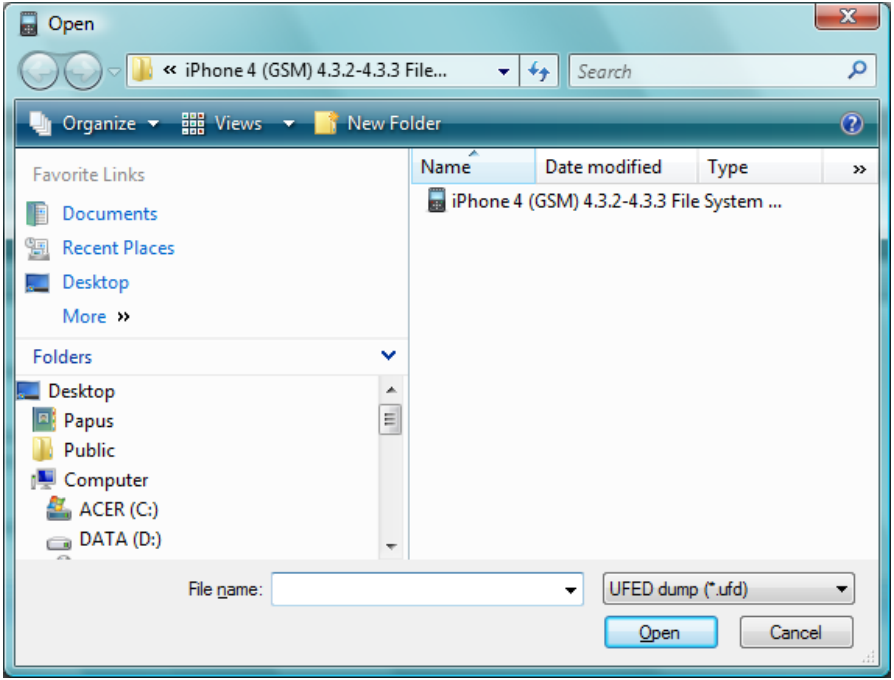
6) Click **Open containing folder**.
7) Copy the **definitions.msd** file to an external storage device, and transfer it to the computer on which UFED Physical Analyzer is installed.
8) Click **Close** to close the Malware Definitions Downloader.

NOTE: To streamline your workflow and save time, it is recommended that you always use the same computer to download the **definitions.msd** file. When you download the **definitions.msd** file to this computer in the future, the Malware Definitions Downloader updates the file instead of downloading the entire file. Make sure that you do not delete the **definitions.msd** file from this computer.

9) In UFED Physical Analyzer, select **Tools** > **Malware Scanner** > **Update signature database**.

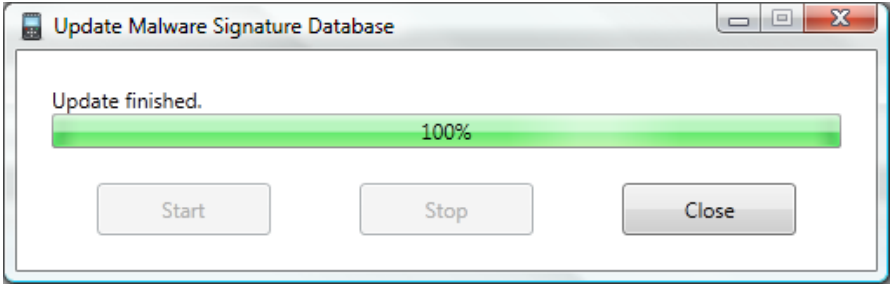

Update Malware Signature Database
You must install the signature database before using the malware scanning for the first time.
Click 'Update from server' to update it from the network
Click 'Update from file' if you already downloaded the database
Idle...
0%
Update from server
Update from file
Close

10) Click **Update from file**.



11) Browse to the malware definitions database file (*.msd), and click **Open**.
12) Click **Start**.

The database is populated.



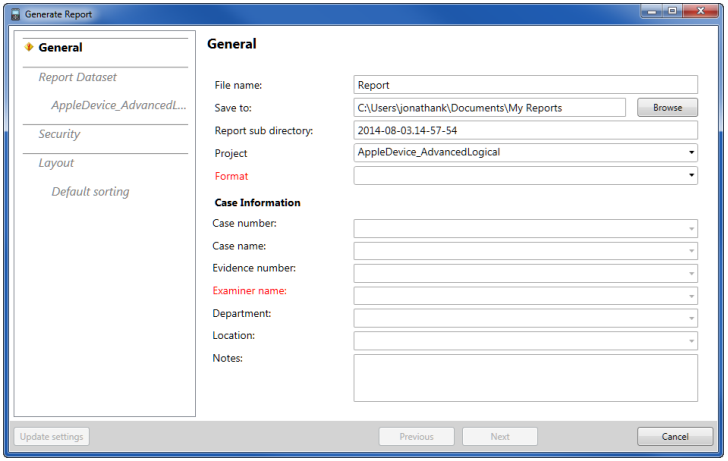
13) Click **Close**.

You can now scan the project for malware.

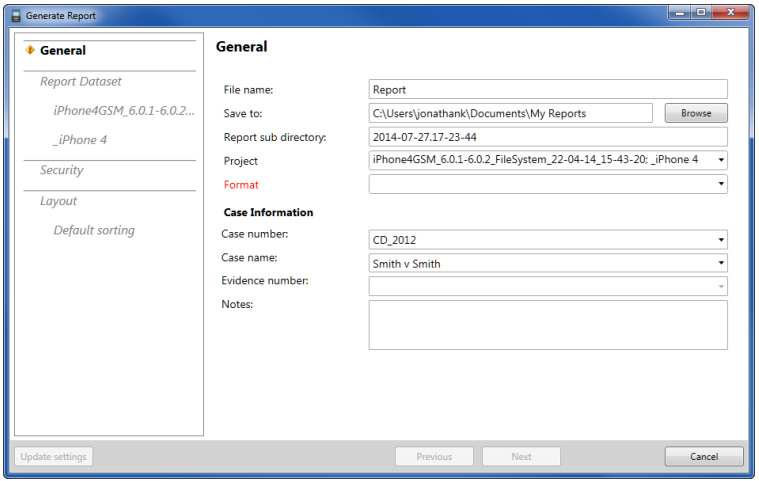
Chapter 9: **Generating a report**

1) You can generate a report of the information in the project. UFED Physical Analyzer provides a report wizard to help you through the steps of creating a report. Do one of the following:
    - Select **Report** > **Generate Report** from the application menu.
    - Click **Generate Report** in the **Extraction Summary** tab.
    - Double-click **Reports** in the project tree.

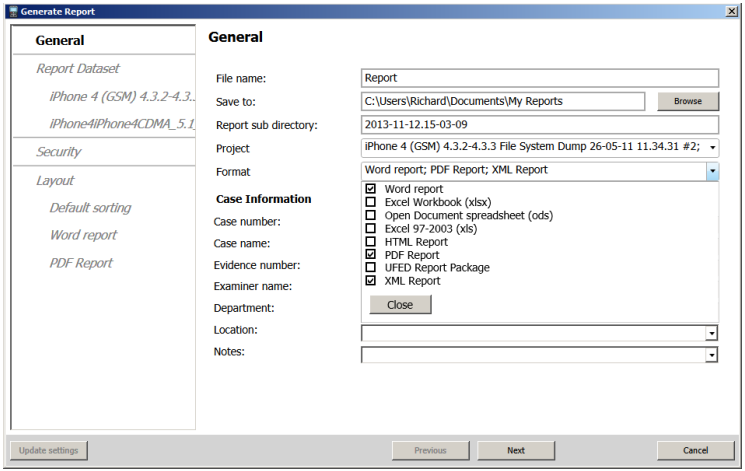
    The Generate Report window appears.



2) In the **File Name**, select the name for the new report you want to create.
3) In the **Save to**, select the folder in which you want to all reports to be created. This folder can be used for all reporting as each report will occupy a separate sub-folder.
4) In the **Report sub-directory** select a name for the folder where you want all selected reports to be created. The default is the current date and time.
5) In the **Project** select the project or projects you want to include in this report. Only projects that are already opened in UFED Physical Analyzer are available for reporting.



6) In the format field choose which of the available formats you want for the report. More than one format can be chosen and a report for each format will be generated.

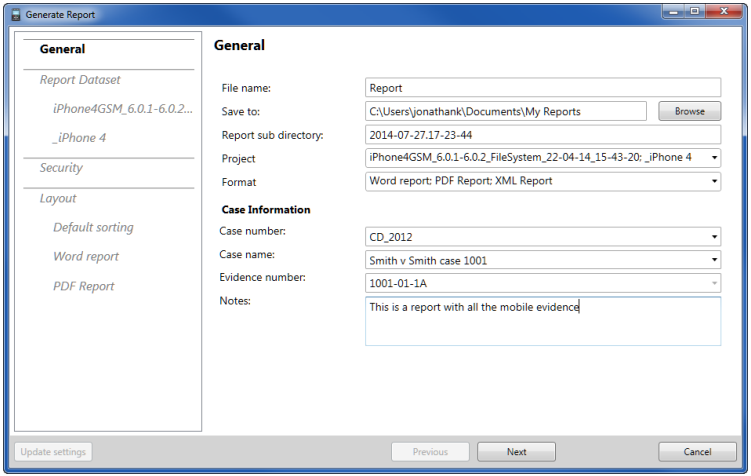


7) In the case information fields you can provide the following:

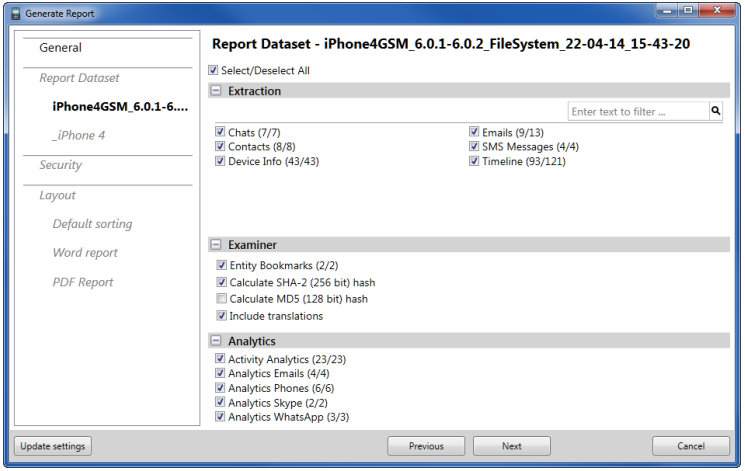
- Case number
- Case name
- Evidence number
- Examiner name
- Department
- Location

NOTE: Default settings for these fields. See *Setting the case information* (page *341*). See *Additional report fields* (page *323*) and *Report defaults* (page *326*) for other defaults. Additionally, the last 10 values entered in these fields are also available in the drop down.

8) Your form should now look like this example:



9) From the following screen select the data to include in the report:

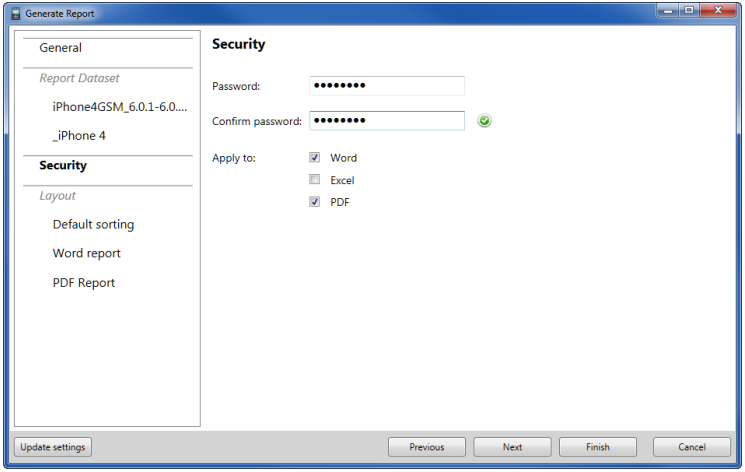


a) **Extraction** - analyzed data and data files to be included in the report.

b) **Examiner** - **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. This selection is for the whole report and applies to all projects within the report. TIP: To shorten the report generation process of large projects do not select these options.
Select **Include translations** to include translated text. The summary table will then include an additional entry – Translated languages, and the translation of the content will appear below the original text with title Translation.

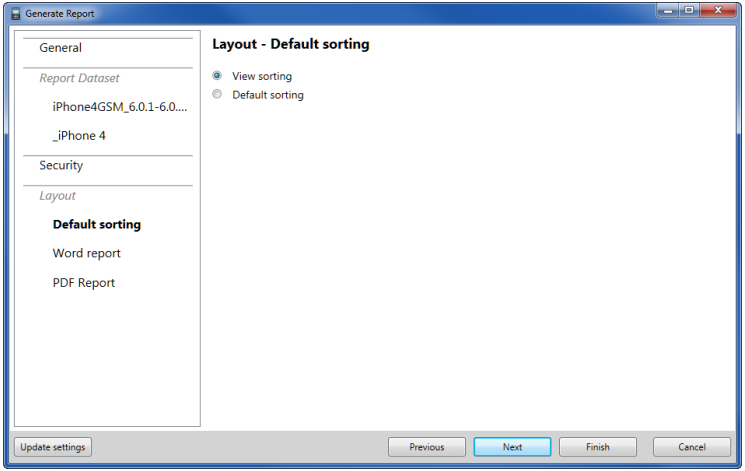
c) **Analytics** - this section appears when there is **Analytics** available in the project. Select the relevant Analytics item(s) to include them in the report.

10) The **security** screen appears. Password protection can be placed on PDF, Word and Excel reports:



Choose the format and provide a password.

11) Select **Default sorting** to sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.



12) For each format chosen for this report you can specify report parameters as follows:

a) Word, HTML and PDF Reports:

- **Disable models categorization** - Select to disable the separation and generate a report in which every data item is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).

- **Logo Header** - Text area where you can enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.
- **Number of messages per chat** - Set the maximum number of messages per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.
- **Font Family** - for PDF reports only.
- **Split HTML report** - for HTML reports only. Ensure that each section of the report starts on a new page.

b) Excel (all formats) and ODS report:

- **The excel report is compatible with OpenOffice** - Select to ensure the Excel report can be opened in OpenOffice.
- **Generate Contact Identification Data** - Select to add a sheet to the Excel report that provides a list of unique contacts based on type.

c) XML and UFED Report package:

- There are NO additional settings required for either of these reports. If the report formats requested only include XML and/or UFED report then no further input is required.

13) Click **Finish**.

NOTE: **Finish** is unavailable until all the required fields are filled. A yellow warning icon is displayed next to all required fields that are not yet complete.

When the report is successfully generated, you are prompted to open the generated report file. The file opens using the associated application to the file format installed in the workstation.

Once a report has been generated for the project, it can be accessed from the Reports section in the project tree. Double click on any of the generated reports to open it in the associated application installed in the workstation. Right click any of the generated reports to open the report file, or select **Open containing folder** to browse the files and folders of the report.

Chapter 10: **Performing extractions**

In UFED Physical Analyzer, perform device extractions in the following ways:

1) For iOS devices, perform advanced logical extraction, physical extraction, file system extraction or Passcode recovery from the device using the iOS Device Extraction application
2) For GPS or mass storage, perform an extraction via UFED Physical Analyzer

10.1. Extraction from iOS devices

Perform a physical or advanced logical extraction from an iPhone, iPod, or iPad device, using iOS Device Extraction.

10.1.1. **Prerequisites**

To perform an extraction from an iOS device, you will need:

- UFED Physical Analyzer installed on a PC
- UFED Cable Number 110 or UFED Cable A with Tip T-110 or Apple 30 pin USB cable supplied with the device

- UFED Cable Number 210 for iOS Logical Extractions from iPhone 5, iPad Mini and iPad4

NOTE: Extraction from iOS devices is not supported in Virtual Machine environments.

In addition, an internet connection is required the first time you run iOS Device Extraction in order to download the necessary support package. Alternatively, the support package can be downloaded using a different computer and copied manually to the computer running iOS Device Extraction. iOS Device Extraction automatically notifies you when a software update is available.

10.1.2. Performing physical extraction

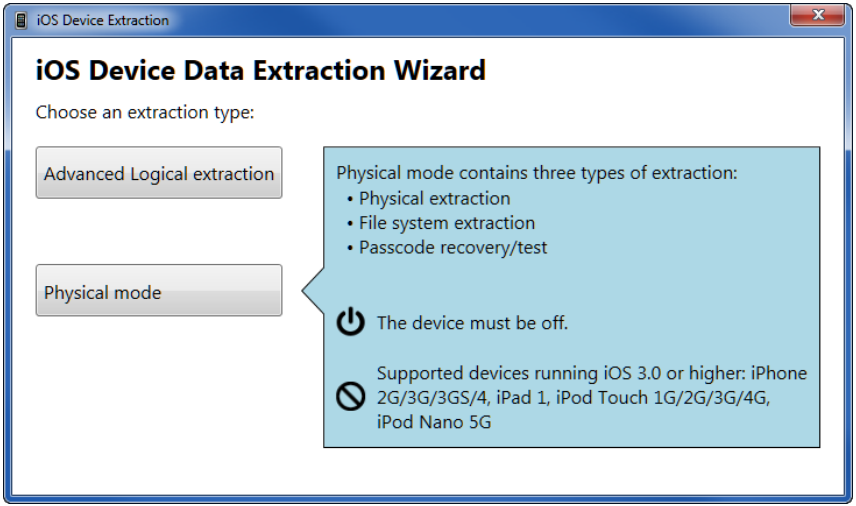
Perform physical and file system extractions from the following devices running iOS version 3.0 or higher:

- iPhone 2G
- iPhone 3G
- iPhone 3GS
- iPhone 4
- iPad 1
- iPod Touch 1G
- iPod Touch 2G

- iPod Touch 3G
- iPod Touch 4G
- iPod Nano 5G

10.1.2.1. Performing physical extraction from non-encrypted iOS devices

1) Select **Extract > iOS Device Extraction** or click to launch iOS Device Extraction.


iOS Device Extraction
iOS Device Data Extraction Wizard
Choose an extraction type:
Advanced Logical extraction
Physical mode
Physical mode contains three types of extraction:
• Physical extraction
• File system extraction
• Passcode recovery/test
The device must be off.
Supported devices running iOS 3.0 or higher: iPhone 2G/3G/3GS/4, iPad 1, iPod Touch 1G/2G/3G/4G, iPod Nano 5G

2) Click **Physical mode**.

   The first time that you run iOS Device Extraction, or when a new support package is available, you are prompted to download the iOS Device Support Package. The support package contains the latest utilities that enable iOS Device Extraction to work with a variety of devices and iOS versions. Depending on your internet connection, the download may take some time.

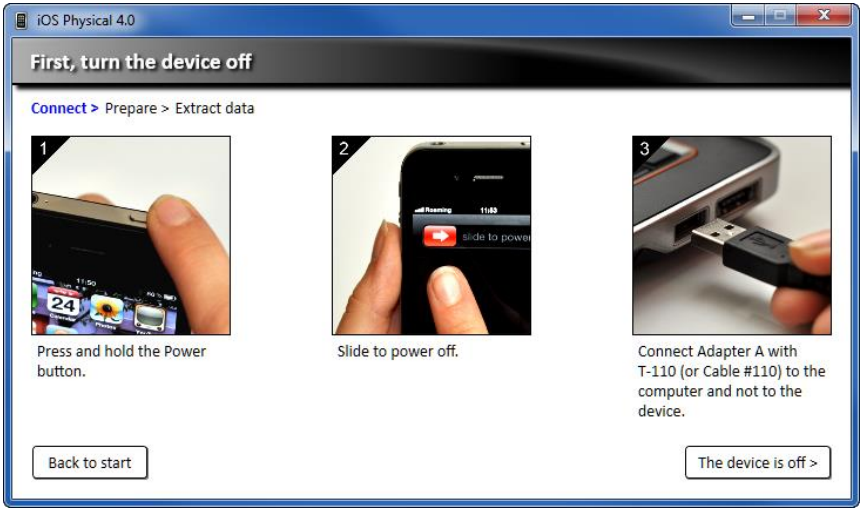
   If your computer is unable to connect to the internet, use a computer with an internet connection to download the latest support package file as follows:

   a) Go to **http://www.cellebrite.com/ios**.

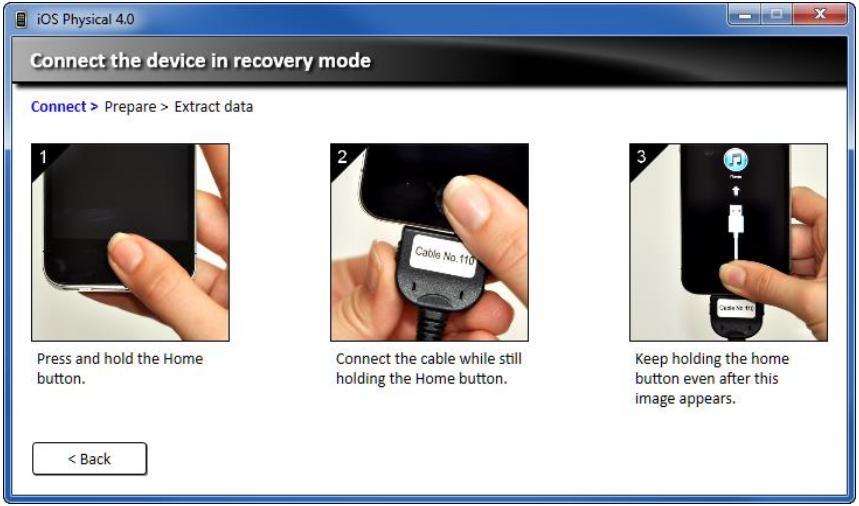
   b) Click **Download**, and save and copy the file to the computer running iOS Device Extraction.

   c) When prompted to install the support package, click **Install from file**, then navigate to the location of the support package file, and click **OK**.

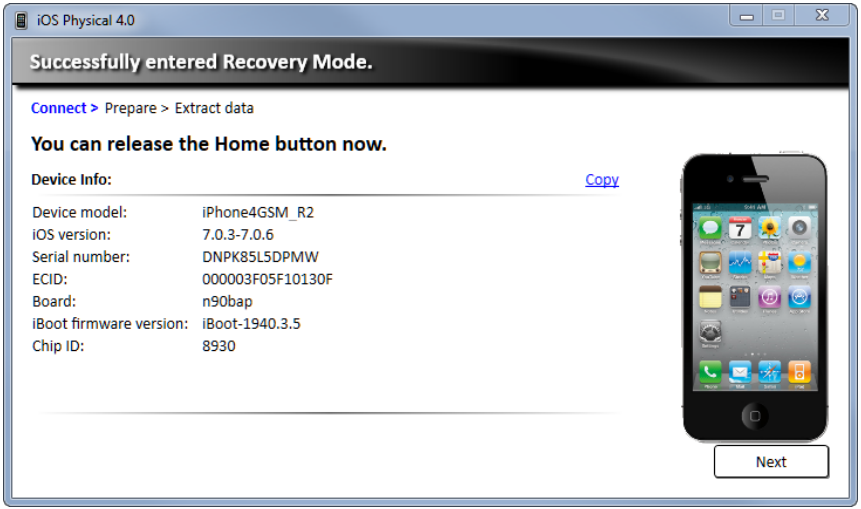
3) Follow the displayed instructions to power off the iOS device and then click **The device is off**.


iOS Physical 4.0
First, turn the device off
Connect > Prepare > Extract data
1
Press and hold the Power button.
2
Slide to power off.
3
Connect Adapter A with T-110 (or Cable #110) to the computer and not to the device.
Back to start
The device is off >

4) Follow the displayed instructions to activate the iOS device in **Recovery Mode**.


iOS Physical 4.0
Connect the device in recovery mode
Connect > Prepare > Extract data
1
Press and hold the Home button.
2
Cable No.110
Connect the cable while still holding the Home button.
3
Keep holding the home button even after this image appears.
< Back

The process automatically continues to the next step.

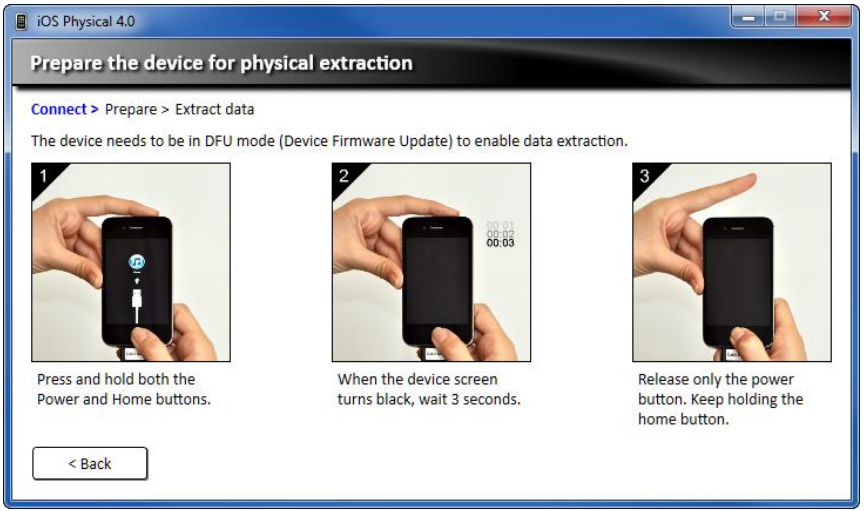


After a device in **Recovery Mode** is detected, iOS Device Extraction displays some device information, such as serial number, hardware version, iOS version and more.

5) If you need this information, click **Copy** to copy the device information to the clipboard.

NOTE: When a range of versions are displayed, the version of the device may be any version within the displayed range. For example, if the version shows **4.0-4.0.2**, the actual version can be 4.0, 4.0.1 or 4.0.2.

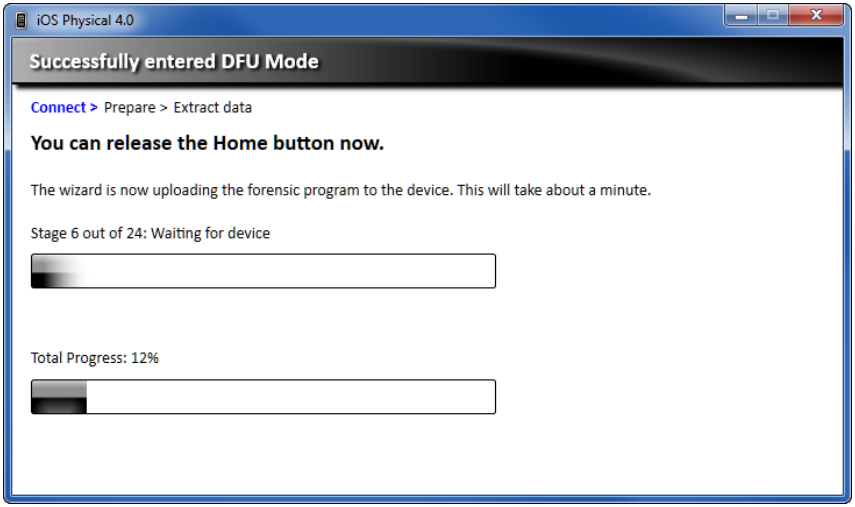
6) Click **Next** to continue.
7) Follow the displayed instructions to set the device to DFU (Device Firmware Upgrade) mode.


iOS Physical 4.0
Prepare the device for physical extraction
Connect > Prepare > Extract data
The device needs to be in DFU mode (Device Firmware Update) to enable data extraction.
1
Press and hold both the Power and Home buttons.
2
00:01
00:02
00:03
When the device screen turns black, wait 3 seconds.
3
Release only the power button. Keep holding the home button.
< Back

iOS Device Extraction does not affect the device firmware or user data.

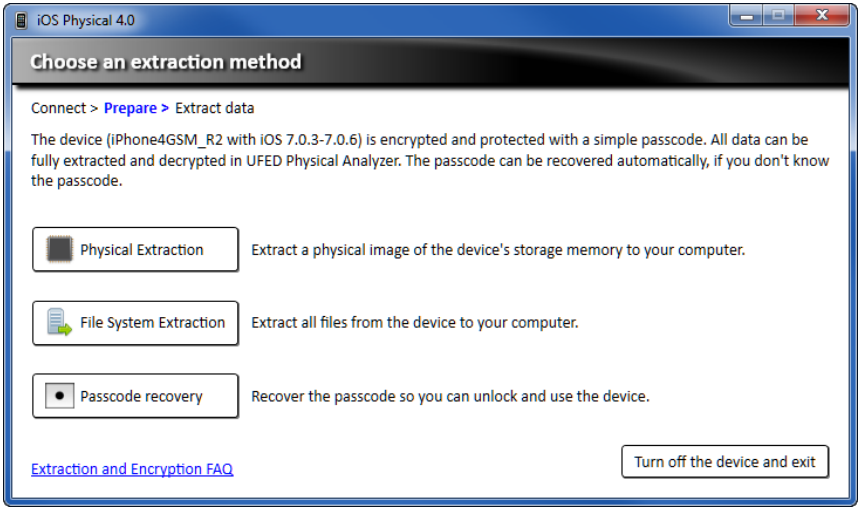
NOTE: This step requires precise timing. If the device accidentally turns on, disconnect it from the cable, turn it off, then go back to step 4.

When the device is in DFU mode, a forensics program required for the extraction automatically uploads to the device.


iOS Physical 4.0
Successfully entered DFU Mode
Connect > Prepare > Extract data
You can release the Home button now.
The wizard is now uploading the forensic program to the device. This will take about a minute.
Stage 6 out of 24: Waiting for device
Total Progress: 12%

The device is now ready for extraction.

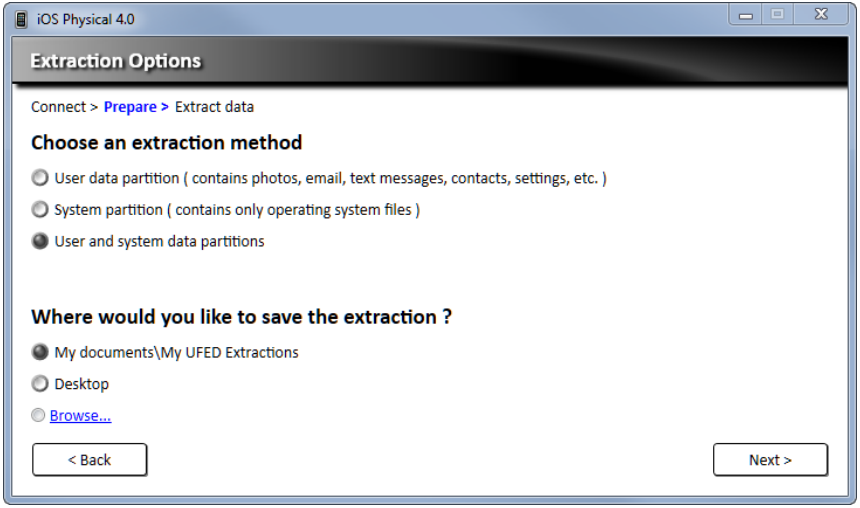
8) Choose the desired extraction type.


iOS Physical 4.0
Choose an extraction method
Connect > Prepare > Extract data
The device (iPhone4GSM_R2 with iOS 7.0.3-7.0.6) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.
Physical Extraction
Extract a physical image of the device's storage memory to your computer.
File System Extraction
Extract all files from the device to your computer.
Passcode recovery
Recover the passcode so you can unlock and use the device.
Extraction and Encryption FAQ
Turn off the device and exit

9) Choose the desired extraction method:

- For Physical Extraction: **User data partition**, **System partition**, or **both**.
- For File System Extraction: **User data partition** or **both**.

Choose the **location** to which to save the extracted data. You can save it locally on the computer or to any removable storage device.


iOS Physical 4.0
Extraction Options
Connect > Prepare > Extract data
Choose an extraction method
User data partition (contains photos, email, text messages, contacts, settings, etc.)
System partition (contains only operating system files)
User and system data partitions
Where would you like to save the extraction ?
My documents\My UFED Extractions
Desktop
Browse...
< Back
Next >

10) Click **Next** to continue.

NOTE: If the device is locked with a passcode, see *Performing physical extraction from encrypted devices* (page *194*).

11) Wait for the extraction process to complete.

The duration varies depending on the extraction method, the device model, the amount of data on the device, the extracting computer, and other parameters.

The following options are available at the end of the extraction process:

- **Open in UFED Physical Analyzer** – Loads the extraction file in UFED Physical Analyzer.
- **Open file location** – Opens the folder that contains the extraction files.
- **Turn off the device and exit** – Turns off the device and sets it back to normal mode.
- **Back to extraction options** – Returns to the extraction methods screen (step 8).

12) Turn off the device and set it back to normal mode.

10.1.2.2. Performing physical extraction from encrypted devices

iOS Device Extraction can extract data from encrypted devices. The amount of data that can be extracted depends on the type of passcode the device is locked with.

There are two kinds of passcodes:

- Simple passcode – 4 digits from 0 to 9 (e.g. 1234, 8787, 2580, etc.)
- Complex passcode – Any combination of numbers, letters and symbols (e.g. 93qP@Mv, iLoVeYoU, etc.)

The decryption process happens in UFED Physical Analyzer and not during the iOS Device Extraction. Most data, such as contacts, messages, photos, some emails, and more, can be decrypted without knowing the passcode. However, to decrypt some of the saved passwords and emails, you need to know the device passcode.

If the device is locked with a simple passcode, iOS Device Extraction automatically recovers the passcode for you. If the device is locked with a complex passcode, you can manually try as many passcodes as you like, or continue the extraction without being able to decrypt some of the saved passwords and emails.

If the device isn't locked with a passcode, all data is extractable – even if the device is encrypted.

10.1.2.2.1. Extracting data from a device with a simple password

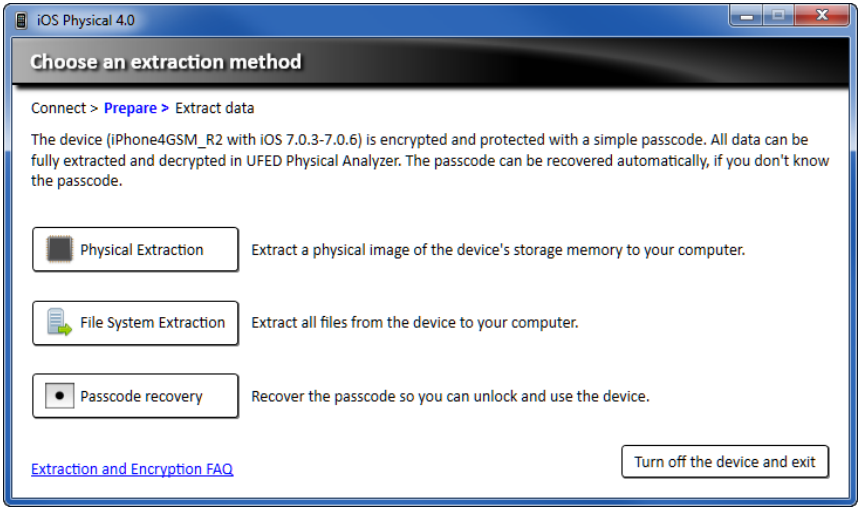
1) Perform steps 1-7 of *Performing physical extraction from non-encrypted iOS devices* (page *185*).

   When the device is ready for extraction (step 8), an additional **Passcode Recovery** option is added to the two extraction options (**Physical Extraction** and **File System Extraction**).

   The Passcode recovery option provides the device passcode so you can unlock and use the device.

2) To extract and recover the passcode in a single process, choose **Physical Extraction** or **File System Extraction**.

The following steps demonstrate a physical extraction process (starting at step 8 of Performing the Data Extraction), but they are the same for a file system extraction.


iOS Physical 4.0
Choose an extraction method
Connect > Prepare > Extract data
The device (iPhone4GSM_R2 with iOS 7.0.3-7.0.6) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.
Physical Extraction
Extract a physical image of the device's storage memory to your computer.
File System Extraction
Extract all files from the device to your computer.
Passcode recovery
Recover the passcode so you can unlock and use the device.
Extraction and Encryption FAQ
Turn off the device and exit

3) Click **Physical Extraction**.
4) Choose the partition you wish to extract, and the location where you want to save the extraction, then click **Next**.
5) If you don't know the passcode, click **Recover the passcode for me** to recover the passcode prior to the extraction.

6) If you know the passcode, enter it in the text box field below. A check mark verifies if the correct passcode was entered.
7) Click **Continue**.

   The extraction process starts.

10.1.2.2.2. Extracting data from a device with a complex password

1) Perform steps 1-7 of *Performing physical extraction from non-encrypted iOS devices* (page *185*).

   When the device is ready for extraction (step 8), an additional **Passcode Recovery** option is added to the two extraction options (Physical Extraction and File System Extraction).

   Use the **Test Passcodes** option to test and verify as many passcodes as you like in real time. iOS Device Extraction cannot recover a complex passcode.

   Most data is decrypted in UFED Physical Analyzer, but some of the saved passwords and email files are not decrypted unless the complex passcode is known.

   The following steps demonstrate a physical extraction (starting at step 8 of Performing the Data Extraction), but they are the same for a file system extraction.

2) Click **Physical Extraction**.
3) Choose the partition you wish to extract and the location to which you want to save the extraction, then click **Next**.

iOS Physical 4.0
The passcode is required for the decryption.
Connect > Prepare > Extract data
Use this option if you don't know the passcode:
Recover the passcode for me >
If you know the passcode, enter it here to save time:
The passcode consist of four digits from 0 to 9.
< Back

4) Do one of the following:
    - If you know the complex passcode, enter it manually. If you do not know the complex passcode, be aware that some data cannot be decrypted by UFED Physical Analyzer.
    - Use the text field to test as many passcodes as you like without locking the device. A check mark appears when you enter the correct passcode.
5) Do one of the following:
    - To start the extraction with the complex passcode, click **Continue >**.
    - To start the extraction without the complex password, click **Continue without passcode**.

The extraction process begins.

10.1.3. Performing advanced logical extraction

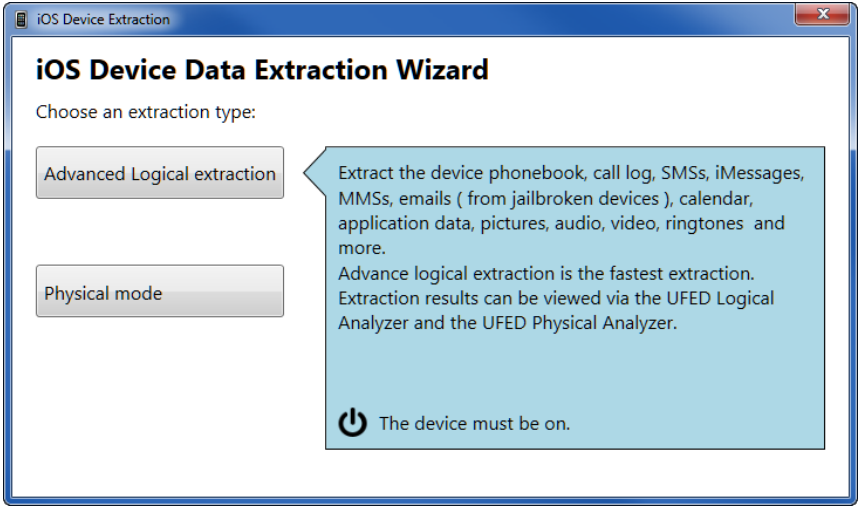
Perform an advanced logical extraction from UFED Physical Analyzer to extract more information than from logical extraction using the UFED unit.

Perform an advanced logical extraction from the following devices:

- iPhone 2G/3G/3GS/4/4s/5/5s/5c
- iPad 1/2/3/4/mini
- iPod Touch 1G/2G/3G/4G
- iPod Nano 5G

10.1.3.1. Performing advanced logical extraction

1) Select **Extract > iOS Device Extraction** or click to launch iOS Device Extraction
2) Click **Advanced Logical extraction**.

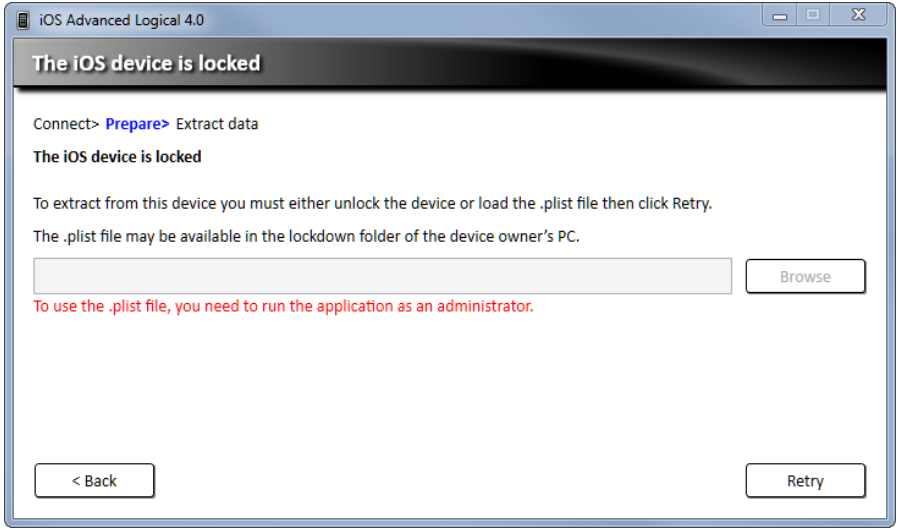

iOS Device Extraction
iOS Device Data Extraction Wizard
Choose an extraction type:
Advanced Logical extraction
Physical mode
Extract the device phonebook, call log, SMSs, iMessages, MMSs, emails (from jailbroken devices), calendar, application data, pictures, audio, video, ringtones and more.
Advance logical extraction is the fastest extraction.
Extraction results can be viewed via the UFED Logical Analyzer and the UFED Physical Analyzer.
The device must be on.

3) Follow the displayed instructions to power on the iOS device and connect the device to your computer, then click **Next**.

NOTE: If the connected device is not recognized, disconnect the device and reconnect it to a USB port at the rear of the PC.

If the iOS device is locked the **Locked Device** screen is displayed. If the .plist file for the locked device is available from the device owner's PC then this .plist file can be loaded in the **Locked Device** screen and then click **Retry.** If the device is locked and no .plist file is available then click **Close.**

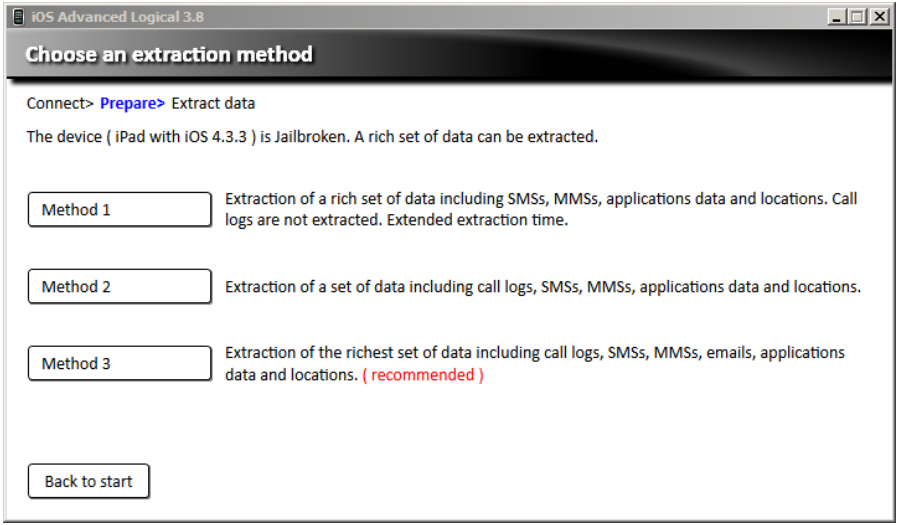
NOTE: To use the .plist file, you need to run the UFED application as an administrator.


iOS Advanced Logical 4.0
The iOS device is locked
Connect> Prepare> Extract data
The iOS device is locked
To extract from this device you must either unlock the device or load the .plist file then click Retry.
The .plist file may be available in the lockdown folder of the device owner's PC.
Browse
To use the .plist file, you need to run the application as an administrator.
< Back
Retry

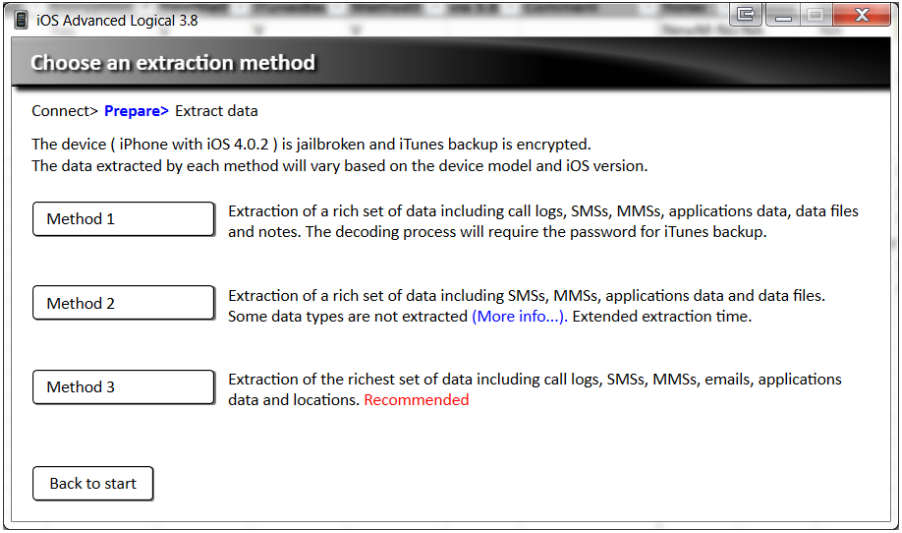
4) Choose a **Method** of Advanced Logical extraction. Depending on whether the device is **jailbroken** and/or **encrypted**, different methods of extraction are made available:
    a) Method 1 - Extraction of a rich set of data including SMSs, MMSs, application data and locations. Call logs, email body and attachments are not extracted. Extended extraction time.
    b) Method 2 - Extraction of a set of data including call logs, SMSs, MMSs, application data and locations. This decoding process may require entering the iTunes backup password.
    c) Method 3 - Extraction of the richest set of data including call logs, SMSs, MMSs, emails, application data, and locations.

In addition the application indicates a specific recommended method per iTunes backup configuration and jailbroken status.

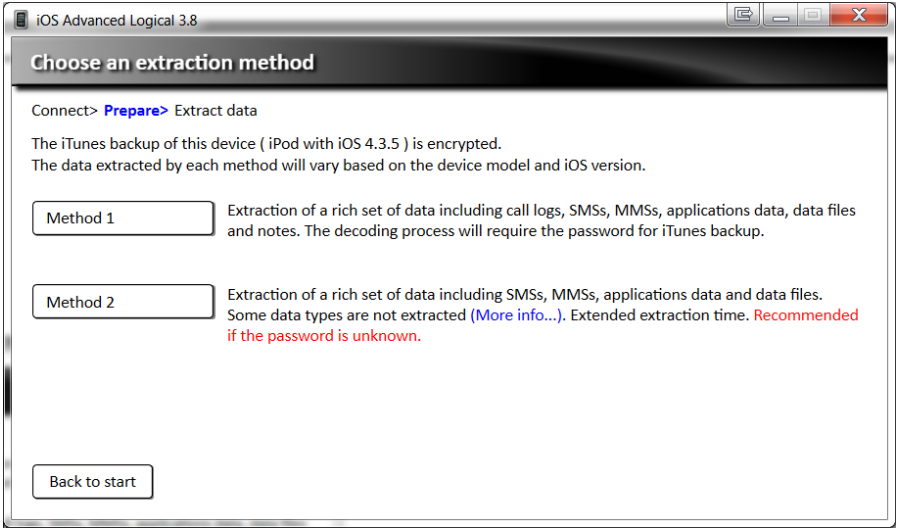
For a **jailbroken** iOS device this screen is displayed -


iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The device (iPad with iOS 4.3.3) is Jailbroken. A rich set of data can be extracted.
Method 1
Extraction of a rich set of data including SMSs, MMSs, applications data and locations. Call logs are not extracted. Extended extraction time.
Method 2
Extraction of a set of data including call logs, SMSs, MMSs, applications data and locations.
Method 3
Extraction of the richest set of data including call logs, SMSs, MMSs, emails, applications data and locations. (recommended)
Back to start

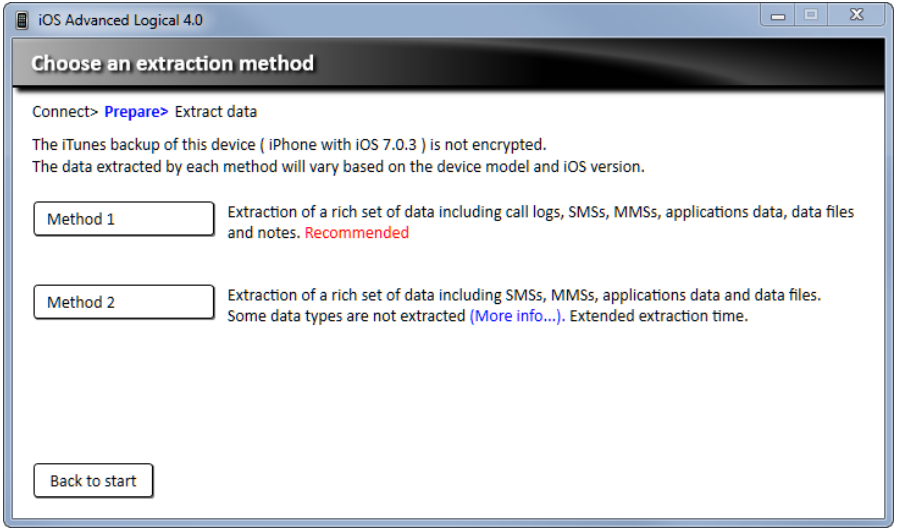
For a **jailbroken encrypted** iOS device this screen is displayed -


iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The device (iPhone with iOS 4.0.2) is jailbroken and iTunes backup is encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup.
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time.
Method 3
Extraction of the richest set of data including call logs, SMSs, MMSs, emails, applications data and locations. Recommended
Back to start

For a **non-jailbroken encrypted** iOS device this screen is displayed -

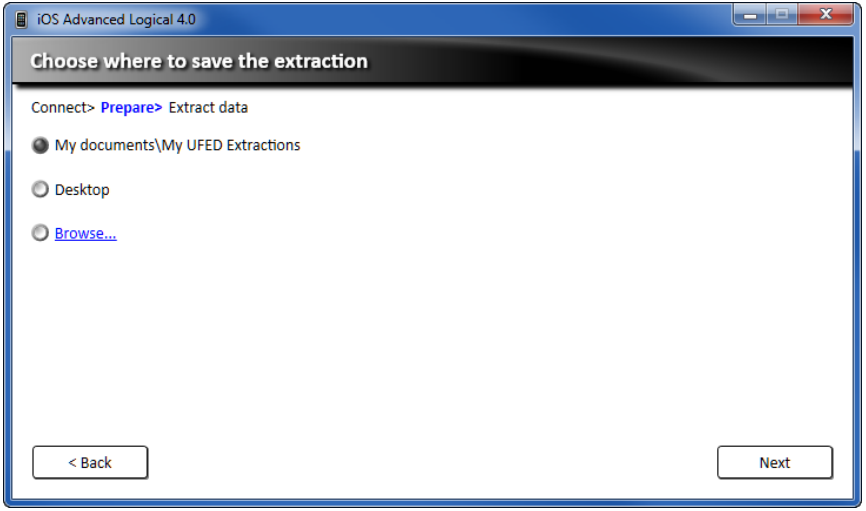

iOS Advanced Logical 3.8
Choose an extraction method
Connect> Prepare> Extract data
The iTunes backup of this device (iPod with iOS 4.3.5) is encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup.
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time. Recommended if the password is unknown.
Back to start

For a **non-jailbroken non encrypted** iOS this screen is displayed

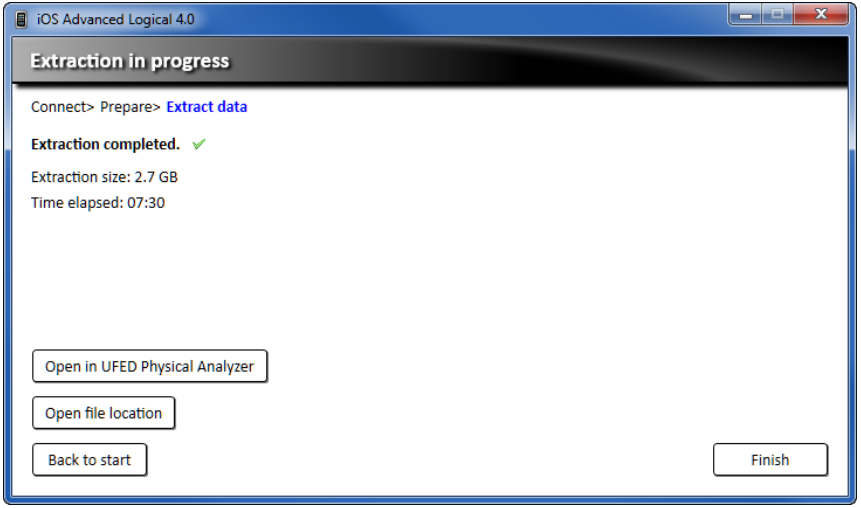

iOS Advanced Logical 4.0
Choose an extraction method
Connect> Prepare> Extract data
The iTunes backup of this device (iPhone with iOS 7.0.3) is not encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. Recommended
Method 2
Extraction of a rich set of data including SMSs, MMSs, applications data and data files. Some data types are not extracted (More info...). Extended extraction time.
Back to start

NOTE: The extraction time will depend on the amount of data on the iOS device and on the method chosen. A **Method 2** extraction from a heavily used device could take several HOURS to complete.

5) Choose the location to save the extracted data. Ensure that there is enough disk space on your chosen location. You can save it locally on the computer or to any removable storage device or to a network location.



6) Click **Next** to continue.
7) A progress bar will be shown. Wait for the extraction process to complete.



NOTE: The duration varies depending on the extraction method, the device model, the amount of data on the device, the extracting computer, and other parameters.

The advanced logical extraction is saved to the selected location as a *.UFD file and a *.TAR file.

Open the advanced logical extraction in UFED Physical Analyzer to access all extracted information, including any deleted information.

NOTE: You cannot access extracted deleted information if you open the extraction in UFED Logical Analyzer.

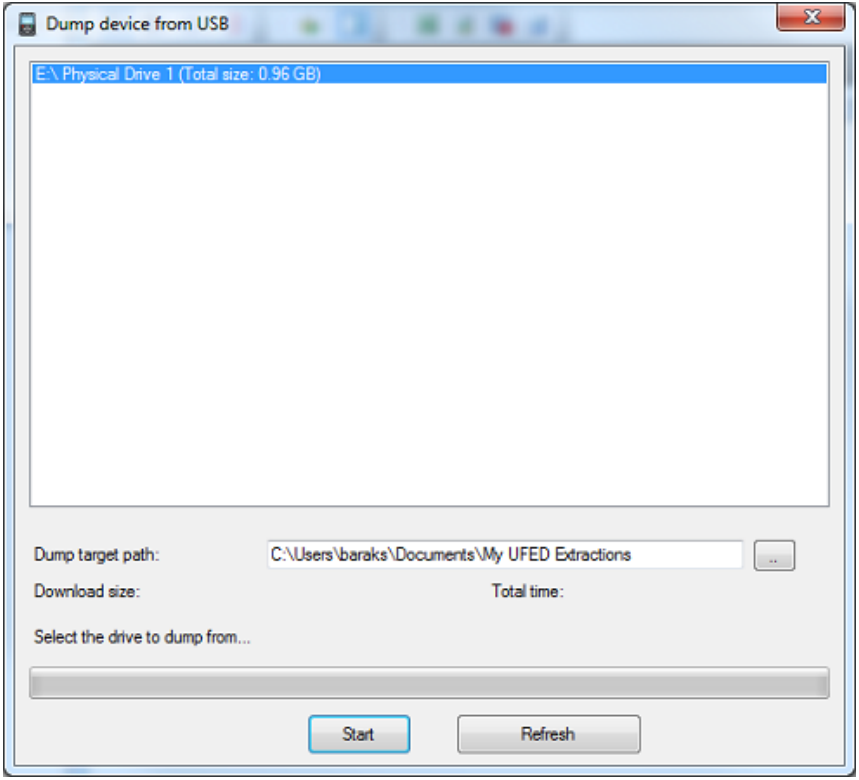
8) Select one of the following options:
   - **Open in UFED Physical Analyzer** – Loads the extraction file in UFED Physical Analyzer.
   - **Open file location** – Opens the folder that contains the extraction files.
   - **Back to start** – Returns to the extraction methods screen.
   - **Finish** – close iOS Device Extraction.

10.2. Extraction from GPS or mass storage devices

Extract and save data from a GPS device (Gamin, Mio, and TomTom) or a mass storage device.

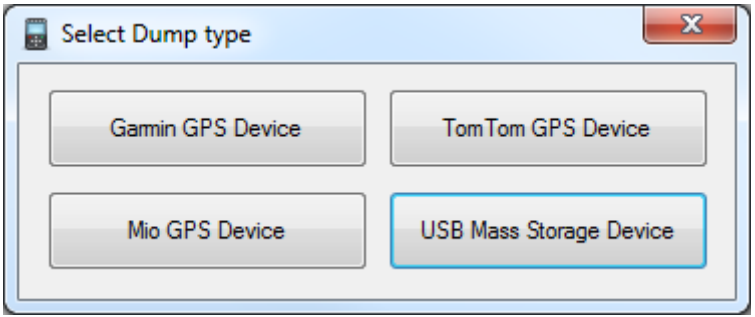
NOTE: Only administrator users can read data from GPS devices. If you are not an administrator, close UFED Physical Analyzer, right-click the UFED Physical Analyzer icon on your desktop, and select **Run as administrator**.

1) Connect the GPS or mass storage device to your PC.
2) Select **Extract** > **Extract GPS/Mass Storage Device**, or click .



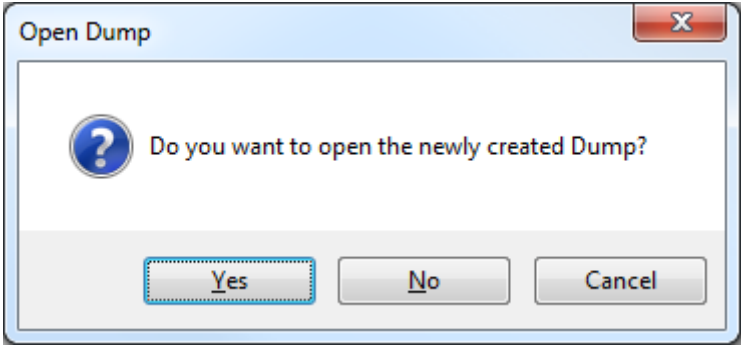
3) Select the device.

4) Do one of the following:
    - Enter the path where you want to save the data extracted from the device.
    - Click ..., and browse to and select the desired location.
5) Click **Start**.



6) Select the type.

The extraction begins. When finished, the following message appears:



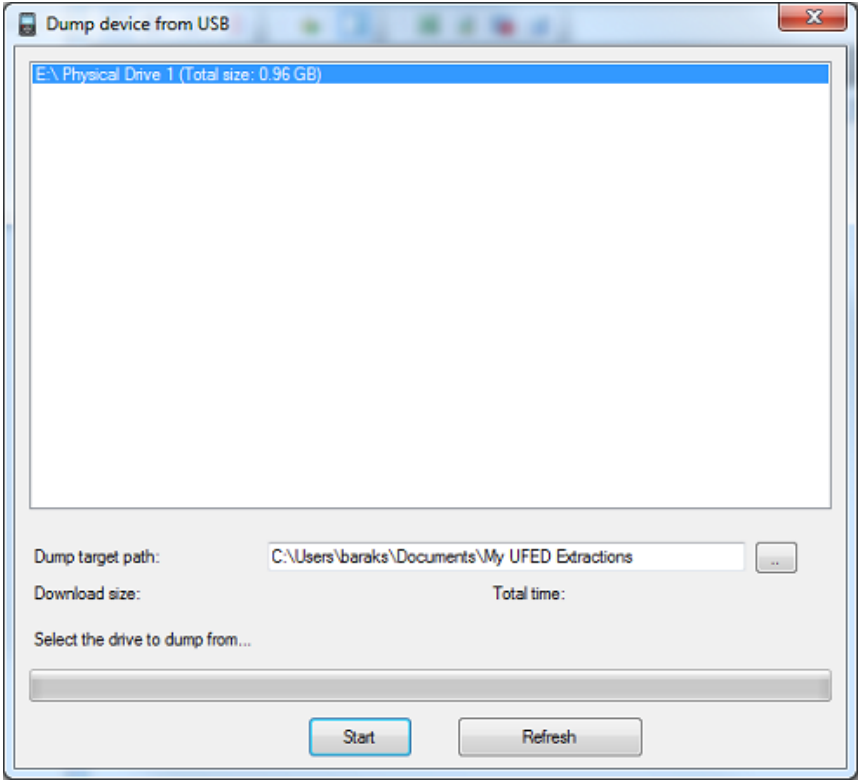
7) Click **Yes** to open the extraction.

10.2.1. Reading data from a GPS or mass storage device

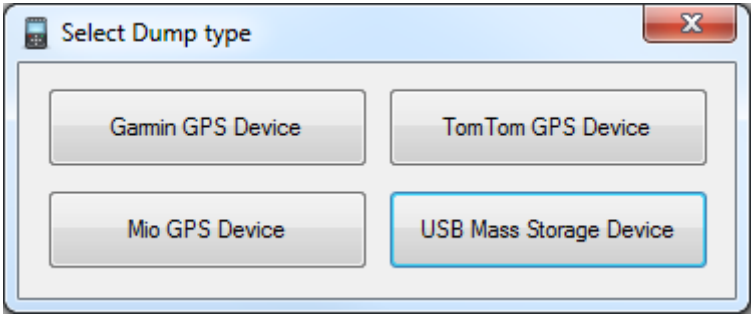
Read and save data from a GPS device (Gamin, Mio, and TomTom) or a mass storage device.

NOTE: Only administrator users can read data from GPS devices. If you are not an administrator, close UFED Physical Analyzer, right-click the UFED Physical Analyzer icon on your desktop, and select **Run as administrator**.

1) Connect the GPS or mass storage device to your PC.
2) Select **Tools** > **Dump GPS/Mass Storage Device**, or click .

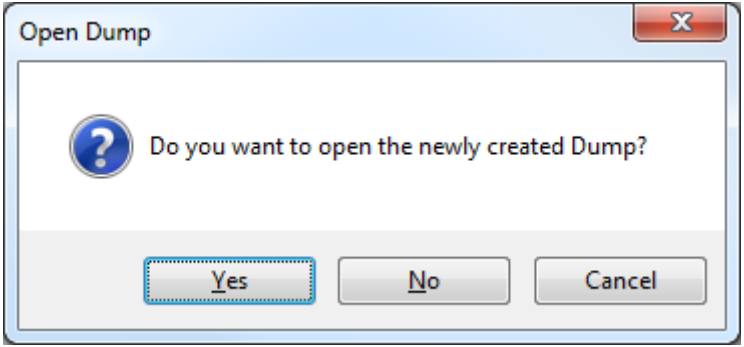

Dump device from USB
E:\ Physical Drive 1 (Total size: 0.96 GB)
Dump target path:
C:\Users\baraks\Documents\My UFED Extractions
...
Download size:
Total time:
Select the drive to dump from...
Start
Refresh

3) Select the device.
4) Do one of the following:
    - Enter the path where you want to save the data extracted from the device.
    - Click ..., and browse to and select the desired location.
5) Click **Start**.



6) Select the dump type.

The extraction begins. When finished, the following message appears:



7) Click **Yes** to open the extraction.

Chapter 11: Advanced features

11.1. Working with TomTom

TomTom generate trip log files that are encrypted by the device only if TomTom users select to share their location information with TomTom. TomTom registers the device location in the trip log files. Export the TomTom XML file generated from the trip logs, and send it to Cellebrite for processing. Once returned, you can view most of the location information available in the file using UFED Physical Analyzer.

For more information on extracting data from a TomTom device, see *Reading data from a GPS or mass storage device* (page *213*).

For more information on geolocations, see *About location data* (page *137*).

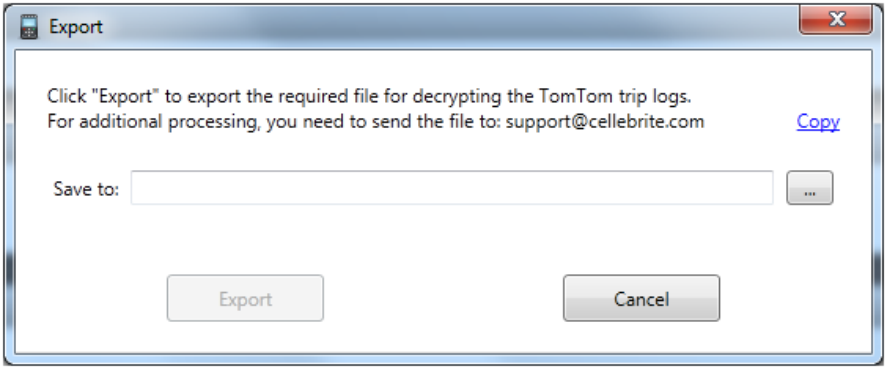
NOTE: Not all the information contained in the TomTom extraction file is retrievable.

NOTE: The processing service can take up to a few days, depending on the volume of data and requests. The service is currently free of charge, but this may be subject to change.

NOTE: You must open the TomTom extraction in UFED Physical Analyzer before exporting or importing the XML file.

11.1.1. Exporting a TomTom file

1) Open an extraction from a TomTom device.
2) In the **Tools** menu, select **TomTom** > **Export**.



3) Browse to the location where you want to save the exported TomTom extraction file, and click **Save**.

   The TomTom extraction file is saved as a GPS.TomTomExport.xml file.

   NOTE: The file does not contain personal user information such as locations.

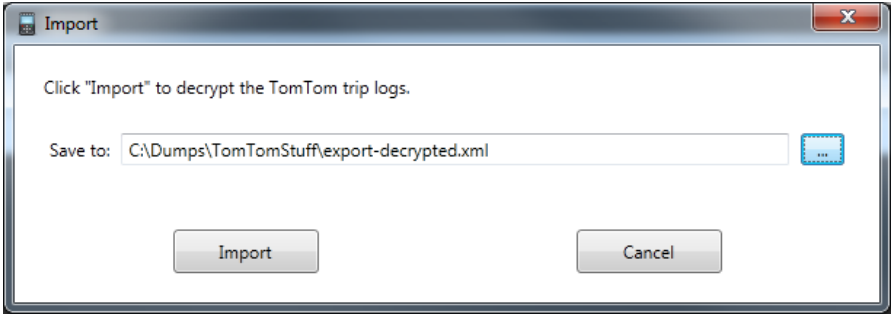
4) Send the GPS.TomTomExport.xml file to: support@cellebrite.com. For US customers: support@cellebriteusa.com.

The GPS.TomTomExport.xml file is processed by Cellebrite support. Your request enters a queue at Cellebrite support. Processing of the TomTom extraction file may take a few days.

11.1.2. Importing a TomTom file

Once Cellebrite support has returned your processed TomTom XML file, import the file to UFED Physical Analyzer.

1) Open the TomTom extraction for which you have the *.xml file.
2) In the **Tools** menu, select **TomTom** > **Import**.



3) Click and browse to the location of the returned TomTom extraction *.xml file, and click **Open**.
4) Click **Import**.

The TomTom *.xml file is imported to UFED Physical Analyzer. The **Locations** tree item is populated.

5) Double-click **Locations** to open the tree item in a data tab.

   The tab shows the device's location at every three seconds with a time and date stamp and geographical coordinates.

NOTE: Not all the information contained in the TomTom extraction file is retrievable.

11.2. Carving images

Perform image carving to retrieve jpeg image files or fragments that are incomplete or corrupt, signifying that they have been deleted by the user. Image carving retrieves the images and rebuilds them as much as possible.

Perform image carving on demand; carving is not performed when UFED Physical Analyzer opens the physical extraction.

NOTE: Image carving is only available for physical extractions.

Image carving is can take some time to process. While processing, you can work in parallel in UFED Physical Analyzer.

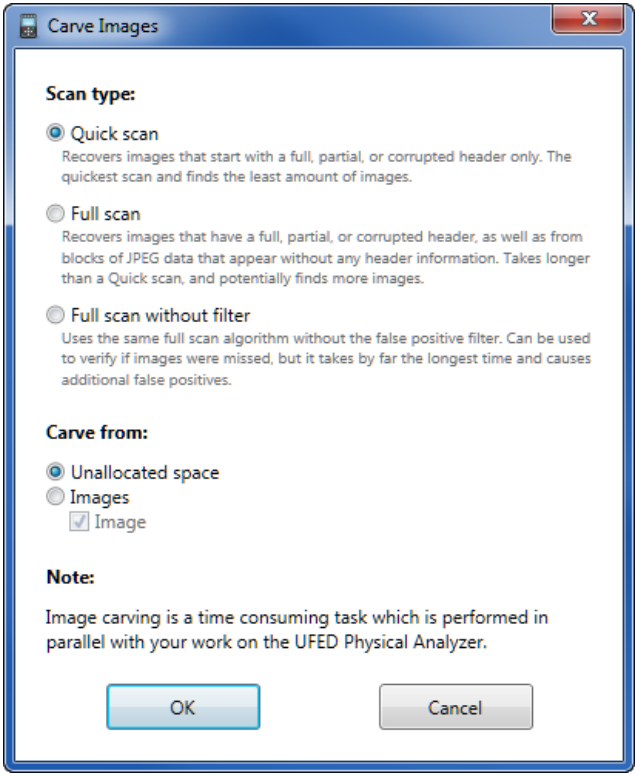
11.2.1. Scanning for carved images

1) Do one of the following:
    - Click .

NOTE: When you click in the toolbar, the scan applies to the active project, that is, the project that you last clicked in.

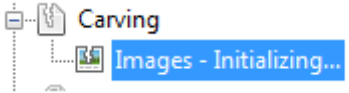
- If you have not scanned for carved images in this session: double-click the **Carving** > **Images** tree item.
- If you have already scanned for carved images in this session: right-click the **Carving** > **Images** tree item and select **Scan again**.

The Carve Images window appears.


Carve Images
Scan type:
Quick scan
Recovers images that start with a full, partial, or corrupted header only. The quickest scan and finds the least amount of images.
Full scan
Recovers images that have a full, partial, or corrupted header, as well as from blocks of JPEG data that appear without any header information. Takes longer than a Quick scan, and potentially finds more images.
Full scan without filter
Uses the same full scan algorithm without the false positive filter. Can be used to verify if images were missed, but it takes by far the longest time and causes additional false positives.
Carve from:
Unallocated space
Images
Image
Note:
Image carving is a time consuming task which is performed in parallel with your work on the UFED Physical Analyzer.
OK
Cancel

2) Select the Scan type:
    - **Quick scan**: This scan has three stages, where UFED Physical Analyzer tries to recover images that start with a full, partial, or corrupted header only.
    - **Full scan**: This scan has five stages, where in addition to recovering images that have a full, partial, or corrupted header, UFED Physical Analyzer tries to recover images from blocks of jpeg data that appear without any header information. A full scan takes longer than a quick scan, and potentially finds more images.
    - **Full scan without filter**: This scan uses the same Full scan algorithm without the false positive filter. It can be used to verify if images were missed, but it takes by far the longest time and causes additional false positives.
3) Select from where you want to carve the images:
    - **Unallocated space**: scan unallocated memory space.
    - **Images**: select all images that you want to scan.
4) Click **OK**.

    The scan begins. Progress is shown next to the **Carving** > **Images** tree item.



11.2.2. Working with carved images

Open data display tabs for all the carved images, for individual carved images, and extract the images to your computer.

To view all the found images in the project tree

- Click ⊞ to expand the **Carving** > **Images** tree item.

To open a data display tab for an individual image:

- Double-click the image in the project tree.

  For more information on working with images, see *Viewing image files* (page *108*).

To extract (dump) the carved images to your computer:

1) Right-click the **Carving** > **Images** tree item and select **Dump**.
2) In the Select Folder window, browse to the desired folder, and click **Select Folder**.

11.3. Verifying hash values

A hash value is a unique and compact representation of a piece of data, which can be used for integrity protection due to the fact that it is computationally improbable to find two distinct inputs that hash to the same value.

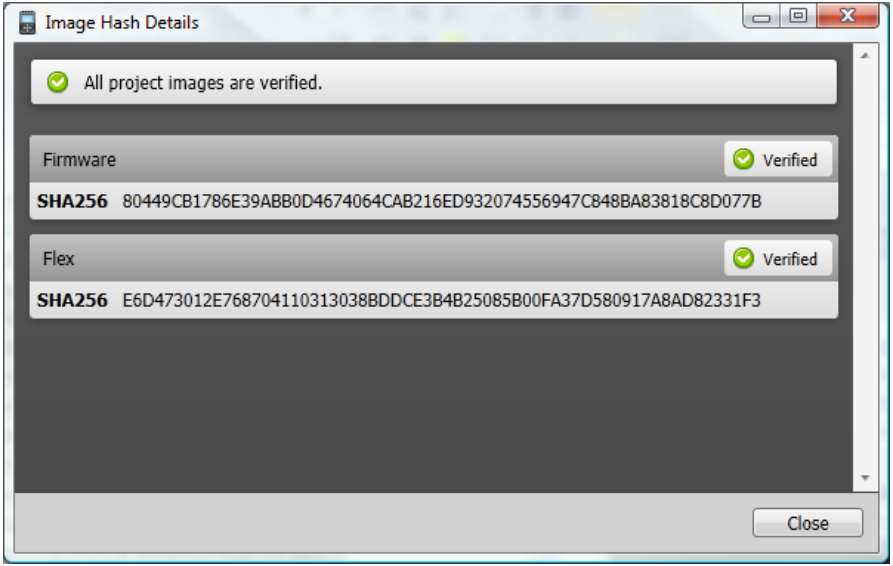
Comparing a reference hash value that was generated during the extraction process for each binary extraction against their calculated hash values enables you to verify the integrity of the binary extractions you received.

To verify the hash values:

1) In the project **Extraction Summary** tab, do one of the following:
    - If hash information is available for the project, click **Verify**.
    - If hash information is not available for the project, click **Calculate hashes**.

    The hash information is calculated or verified. If no reference data is available, a **Hashes have been calculated for this project, but no reference data is available** message is displayed in the **Image Hash Information** section of the **Extracted** Summary tab.

2) Click **Show Details**.



The Image Hash Details dialog displays the comparison result of the reference and calculated hash values of each image.

- Verified indicates matching values.
- Bad Verification indicates the images do not match.

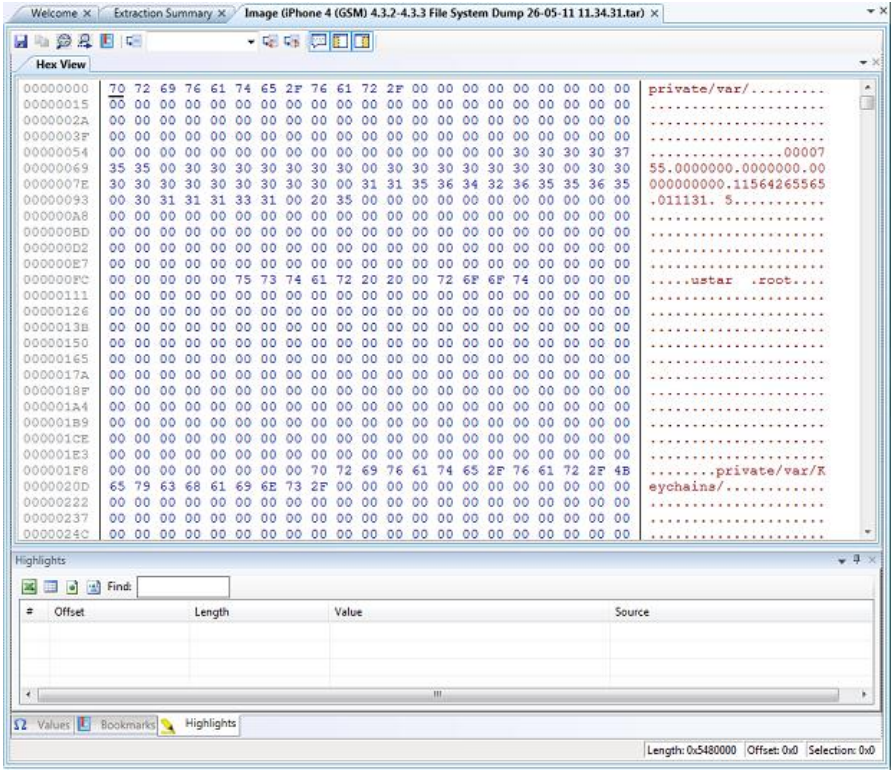
Chapter 12: **Working with hex data**

The extraction enables you to view the device image, which is a single file or multiple files that contain a comprehensive copy of the contents and structure of the data on the device.

To access the hex view of the device image:

- In the project tree, expand the **Images** tree item, and double-click the desired image.

An Image tab appears in the data display area showing the image data in Hex view.

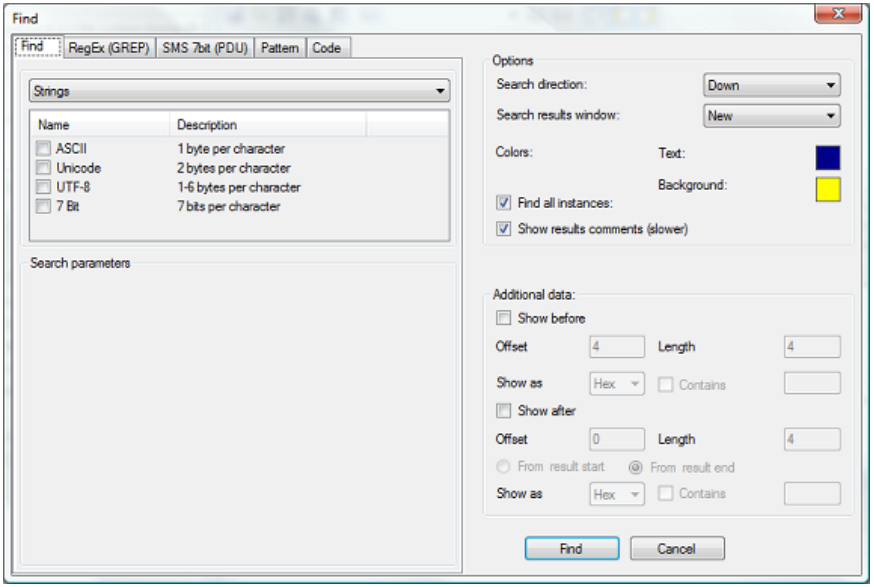


Located under the Hex view tab are Analysis Information tabs that display the following types of information related directly to the displayed Hex data:

- **Values** - A wide array of value interpretations, such as 8, 16, 32, and 64 bit, various string encoding, date & time formats, and more, calculated on the fly for the currently selected data in the Hex view. See *Working in the Values tab* (page *104*).
- **Bookmarks** - A list of bookmarks added in the displayed Hex data. See *Working with bookmarks* (page *276*).
- **Highlights** - A list of content segments markups highlighted in the displayed Hex data. The number of highlight results is shown in brackets next to the tab name. See *Working in the Highlights tab* (page *106*).
- **Search** - Displays results of a search in the displayed Hex data. A new search results tab opens for each search query performed. The number of results for each search is shown in brackets next to the tab name.

For more information on the Image tab, see *Hex view* (page *100*).

12.1. Searching for information in the Hex data and decoded data



The Find window has several tabs that enable you to search the Hex data in the following modes:

- **Find** - Search for specific parameters, such as strings, bytes, dates, and more.
- **RegEx (GREP)** - Search for strings using Regular Expressions.
- **SMS 7Bit (PDU)** - Search for SMS text strings.
- **Pattern** - Search for text patterns, in cases in which the pattern of the text is understood but not the text itself (mainly used for 7 bit search to locate SMS messages).
- **Code** - Specialized search for user codes and passwords.

NOTE: The **Find** modes were built using the Plug-ins architecture. The find options can be enhanced and extended by adding new search plug-ins.

For more information on targeted searches, refer to the following sections:

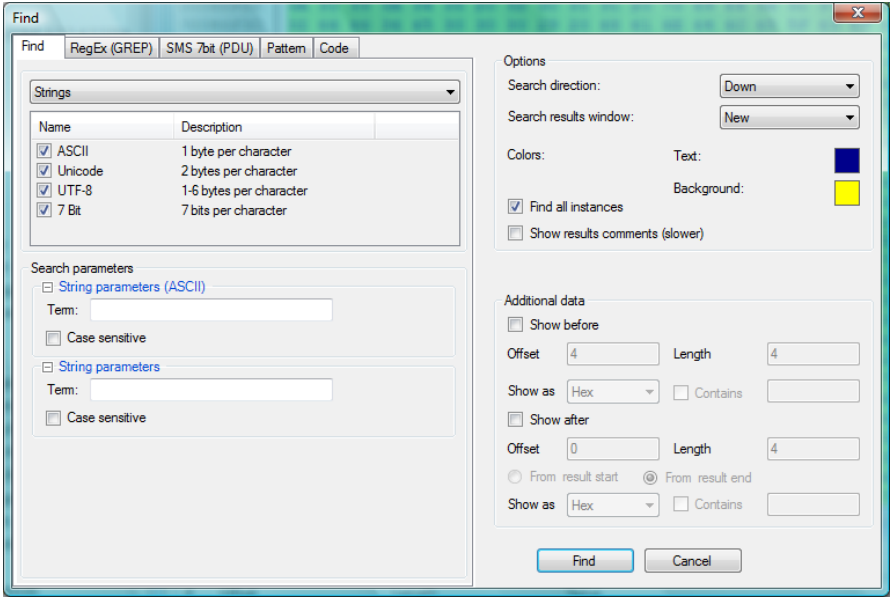
- *Searching strings* (page *232*)
- *Searching bytes* (page *237*)
- *Searching dates* (page *241*)
- *Searching SIM ICCID numbers* (page *246*)
- *Searching SMS numbers* (page *251*)
- *Searching for regular expressions (GREP)* (page *255*)

- *Searching SMS text strings* (page *260*)
- *Searching for patterns* (page *265*)
- *Searching for codes and passwords* (page *270*)

12.1.1. Searching strings

Search for strings to locate different types of data in the Hex data, e.g. text messages, phone numbers, names or any other string data.

1) While viewing Hex data, click to open the Find window.
2) In the **Find** tab, select **Strings** from the data type list.



3) Select the type of text encoding to search for the given string:
   - **ASCII**
   - **UNICODE** (mainly for non-Latin characters)
   - **UTF-8**
   - **7 bits** (mainly for SMS text)

The **Search parameters** area appears.

4) In the **Search parameters** area:
   a) In the **Term** box in the **String parameters** area, enter the search string.
   b) Select the **Case sensitive** option, if necessary.
5) In the **Options** area, set the desired search options:
   a) In the **Search direction** list, select the search direction.
   b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d) Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

6) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

   a) Select **Show before** to show the data immediately before what you are searching for.

   b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

   c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

   d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

   e) Select **Contains**, and enter a string that the search result must contain in its additional data.

   f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

   g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

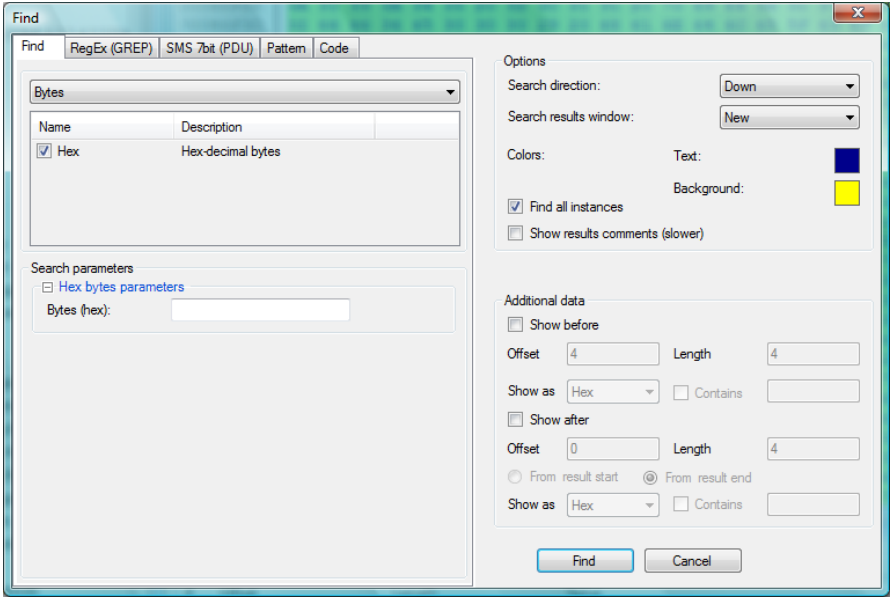
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9) To search for specific data and filter the search results, use the **Find** box in the search results tab.
10) To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.2. Searching bytes

Search for bytes to look for specific occurrences in the Hex data. This is especially useful when you know the identifying header of a file type or information you are looking for. For example, the starting Hex bytes of a jpeg image are **FF D8 FF**. Therefore, the result of searching for **FF D8 FF** provides the locations of all possible jpeg image headers in the Hex data.

1) While viewing Hex data, click to open the Find window.
2) In the **Find** tab, select **Bytes** from the data type list.



3) Select **Hex**.

   The **Search parameters** area appears.

4) In the **Bytes (hex)** box, enter the Hex value, for example, **FFD8FF**.
5) In the **Options** area, set the desired search options:

a) In the **Search direction** list, select the search direction.

b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.

c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

6) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

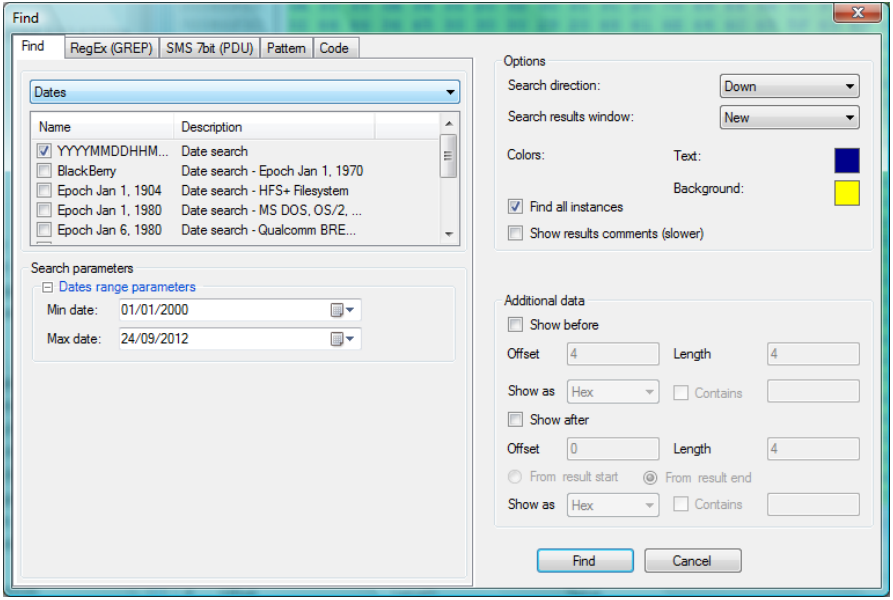
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9) To search for specific data and filter the search results, use the **Find** box in the search results tab.
10) To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.3. Searching dates

Search for dates to find date ranges in the Hex data.

1) While viewing Hex data, click to open the Find window.
2) In the **Find** tab, select **Dates** from the data type list.



The filter box displays a list of date formats and plug-ins that can be used for date searches.

3) Select the desired date format(s) and any plug-in(s) that you want to use in the current search.

NOTE: What plug-ins are suitable depend on how the data is encoded, what type of device you are analyzing, and so on. If you select a plug-in that is not suitable, your search results may contain false results. For example, you can select **BlackBerry** if you are analyzing a BlackBerry device. If you are not analyzing a BlackBerry device, selecting **BlackBerry** may return results that are inaccurate.

The **Search parameters** area appears.

4) In the **Min Date** and **Max Date** fields, click to select a date from the calendar.

Tip: Set a short date range in order to reduce the number of given results.

Tip: When searching for a particular date, set the **Min Date** and **Max Date** fields to a range of not less than 24 hours.

5) In the **Options** area, set the desired search options:

   a) In the **Search direction** list, select the search direction.

   b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.

   c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

   The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

6) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.

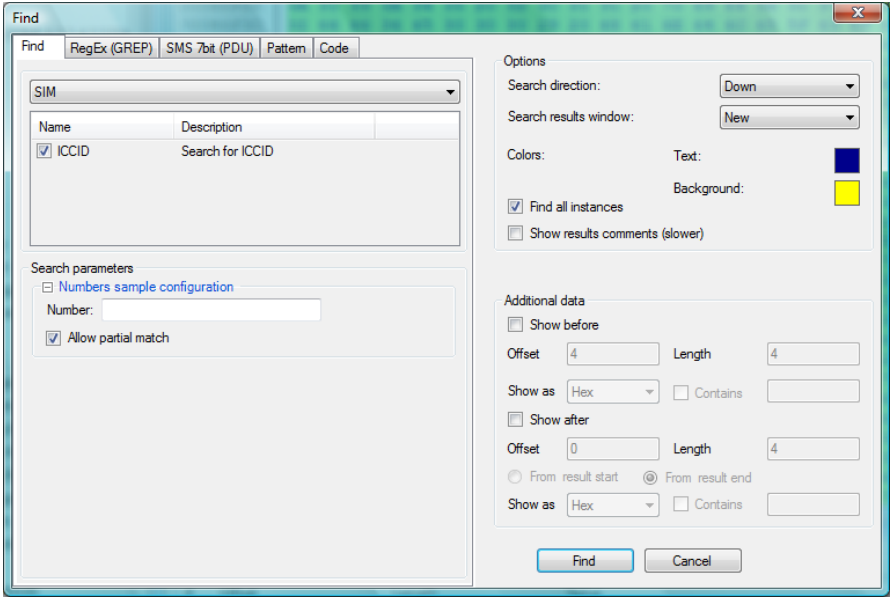
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9) To search for specific data and filter the search results, use the **Find** box in the search results tab.
10) To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.4. Searching SIM ICCID numbers

This search method enables you to search for SIM ICCID numbers in the Hex data.

1) While viewing Hex data, click to open the Find window.
2) In the **Find** tab, select **SIM** from the data type list.



3) Select **ICCID**.

   The **Search parameters** area appears.

4) In the Numbers sample configuration area, enter the ICCID number in the **Number** box.

5) If you entered only part of the number, select **Allow Partial Match**. For example, entering the number **89972** and selecting this option, UFED Physical Analyzer searches for ICCID numbers provided by an Israeli service provider.
6) In the **Options** area, set the desired search options:
    a) In the **Search direction** list, select the search direction.
    b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
    c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

    The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

    Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
    d) Do one of the following:
        - Select **Find all instances** to display all search results at the end of the process
        - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
    e) Select **Show results comments** to display

7) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

   a) Select **Show before** to show the data immediately before what you are searching for.

   b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

   c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

   d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

   e) Select **Contains**, and enter a string that the search result must contain in its additional data.

   f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

   g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

   The additional data is logged to the **Additional before** and **Additional after** fields of search results.

8) Click **Find**.

   NOTE: If the **Number** field is left empty, the search results include all the numbers that match the ICCID format.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

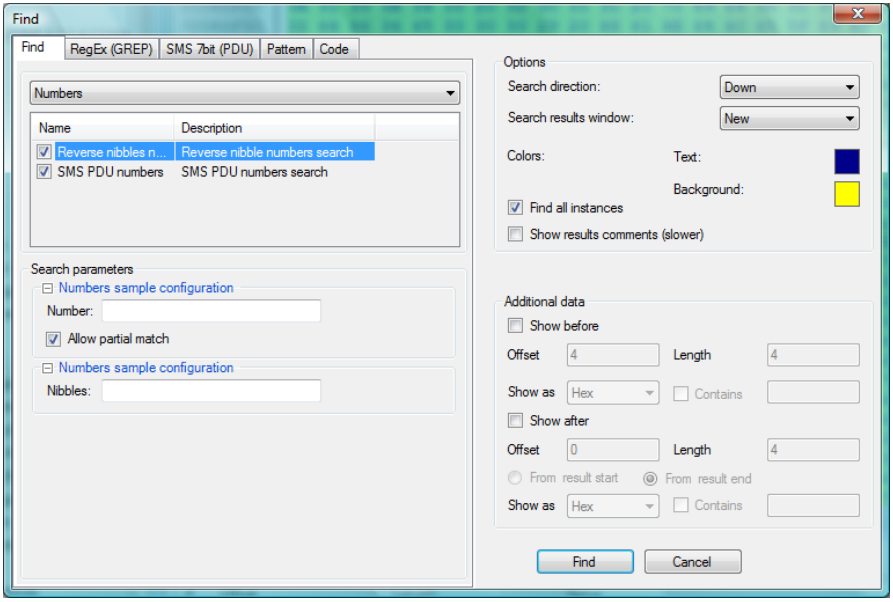
- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

9) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
10) To search for specific data and filter the search results, use the **Find** box in the search results tab.
11) To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.5. Searching SMS numbers

Search for SMS numbers in the Hex data.

1) While viewing Hex data, click to open the Find window.
2) In the **Find** tab, select **Numbers** from the data type list.



3) To perform a search of SMS PDU numbers, select **SMS PDU numbers**.

   The **Search parameters** area appears.

   a) In the **Number** field, enter the search number.

   NOTE: If the **Number** field is left empty, the search results include all the numbers that match the SMS Number format.

   b) If you entered only part of the number, select **Allow Partial Match**.

4) To a search for reversed nibbles, select **Reverse nibbles numbers**.

   NOTE: Use this option when the data has been encoded to include reversed nibbles.

   The **Search parameters** area appears.

   - In the **Nibbles** field, enter the desired nibble.

5) In the **Options** area, set the desired search options:

   a) In the **Search direction** list, select the search direction.

   b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.

   c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

6) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**

- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

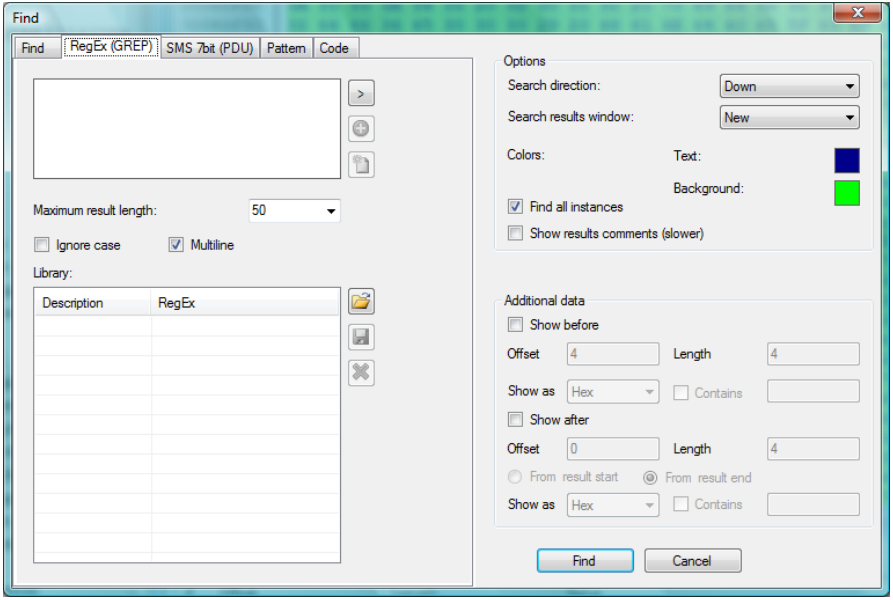
8) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9) To search for specific data and filter the search results, use the **Find** box in the search results tab.
10) To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.1.6. Searching for regular expressions (GREP)

Search for regular expressions to (RegEx) in order to look for a specific string structure within the data.

For example, the regular expression "**[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[A-Za-z]{2,4}**", UFED Physical Analyzer searches your data for all the email addresses that match the structure **<string>@<string>.<2 to 4 letters>**.

1) While viewing Hex data, click to open the Find window.



2) In the **RegEx (GREP)** tab, enter the expression that you want to use in the search.

3) Click to enter a regular expression code from a list of common codes..

4) Click to save the current expression in the library list.

5) Click to clear the regular expression field.
6) Set the **Maximum result length** value to filter only results that are up to the specified length.
7) Select **Ignore case** to disregard the case in the search results.
8) Select **Multiline**.
9) To use a saved expression from the library, click it in the **Library** area.
10) To export the current regular expression library to a *.rel file, click .
11) To load an exported regular expression from a *.rel file, click .
12) To delete an expression from the library list, click .
13) In the **Options** area, set the desired search options:
    a) In the **Search direction** list, select the search direction.
    b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
    c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

    The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

14) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

15) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.

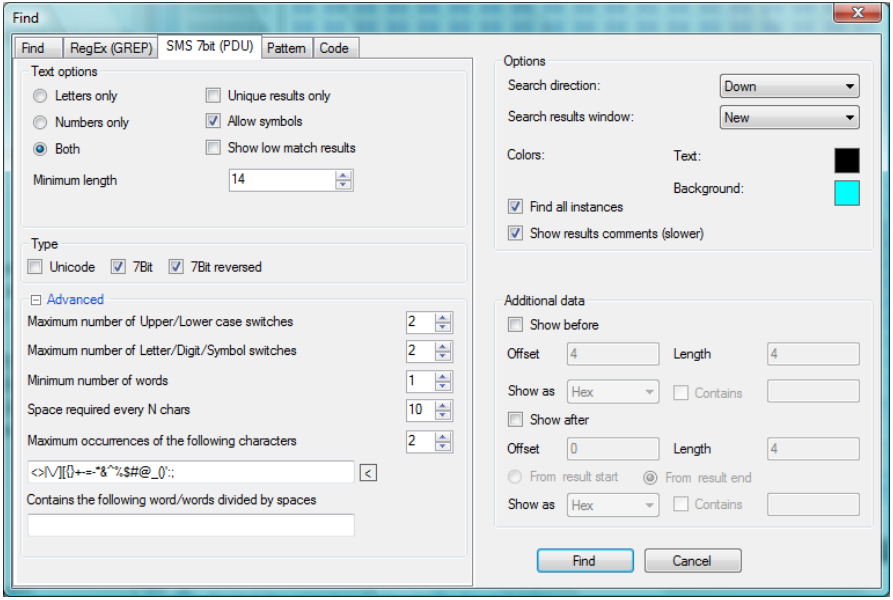
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

16) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
17) To search for specific data and filter the search results, use the **Find** box in the search results tab.
18) To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.7. Searching SMS text strings

This search method enables you to search for SMS text strings (7bit PDU) in the Hex data

1) While viewing Hex data, click to open the Find window.
2) Select the **SMS 7Bit (PDU)** tab.



3) In the **Text Options** area, set the following search parameters:
    a) Set the search type: **Letters only**, **Numbers only**, or **Both**.
    b) To show unique results, select **Unique results only**.
    c) To allow symbols in the search results, select **Allow symbols**.

d) To show low match results, select **Show low match results**.

e) To set the minimum number of characters in the results, set the **Minimum length**.

4) In the **Type** area, select the search type: **Unicode**, **7Bit**, **7Bit reversed**.

5) In the **Advanced** area, set the following, as applicable:

- **Maximum number of Upper/Lower case switches**
- **Maximum number of Letter/Digit/Symbol switches**
- **Minimum number of words**
- **Space required every N chars**
- **Maximum occurrences of the following characters**
- **Contains the following words divided by space**s.

6) In the **Options** area, set the desired search options:

a) In the **Search direction** list, select the search direction.

b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.

c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

7) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

8) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.

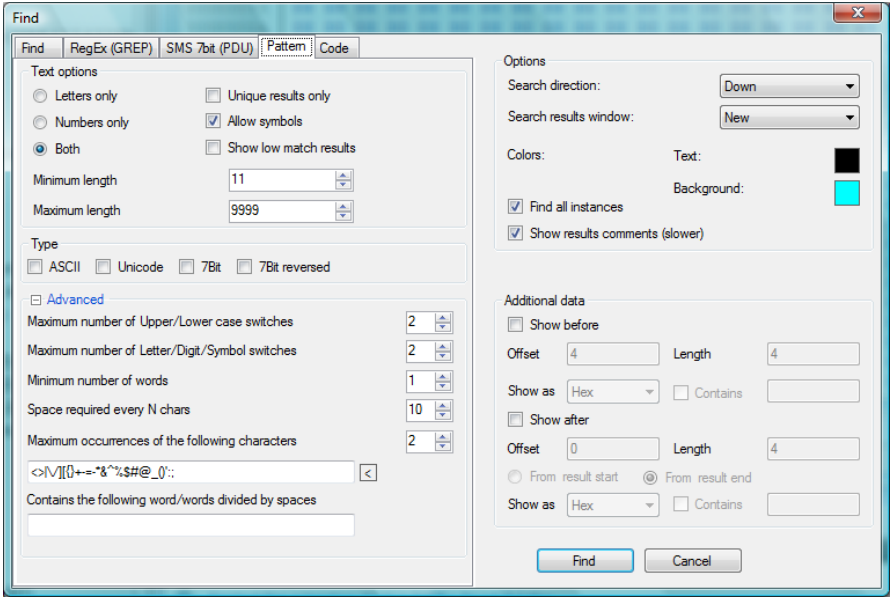
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

9) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
10) To search for specific data and filter the search results, use the **Find** box in the search results tab.
11) To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.8. Searching for patterns

When navigating within a large memory structure, the search for patterns to locate any content that is textual in nature.

1) While viewing Hex data, click to open the Find window.
2) Select the **Pattern** tab.



3) In the **Text Options** area, set the following search parameters:
    a) Set the search type: **Letters only**, **Numbers only**, or **Both**.
    b) To show unique results, select **Unique results only**.
    c) To allow symbols in the search results, select **Allow symbols**.

d) To show low match results, select **Show low match results**.

4) In the **Minimal length** and **Maximal length** fields, set the pattern length range.

   This option enables you to filter the results according to the searched patterns.

5) In the **Type** area, select the search type: **ASCII**, **Unicode**, **7Bit** and/or **7Bit reversed**.

6) In the **Advanced** area, set the following, as applicable:

   - **Maximum number of Upper/Lower case switches**
   - **Maximum number of Letter/Digit/Symbol switches**
   - **Minimum number of words**
   - **Space required every N chars**
   - **Maximum occurrences of the following characters**
   - **Contains the following words divided by space**s.

7) In the **Options** area, set the desired search options:

   a) In the **Search direction** list, select the search direction.

   b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.

   c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

   The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.

d) Do one of the following:

- Select **Find all instances** to display all search results at the end of the process
- Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).

e) Select **Show results comments** to display

8) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

9) Click **Find**.

NOTE: Pattern search can be used to locate all possible 7 bit SMS text results. To minimize the number of false positive results set the **Minimal Length** value to a higher number.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**

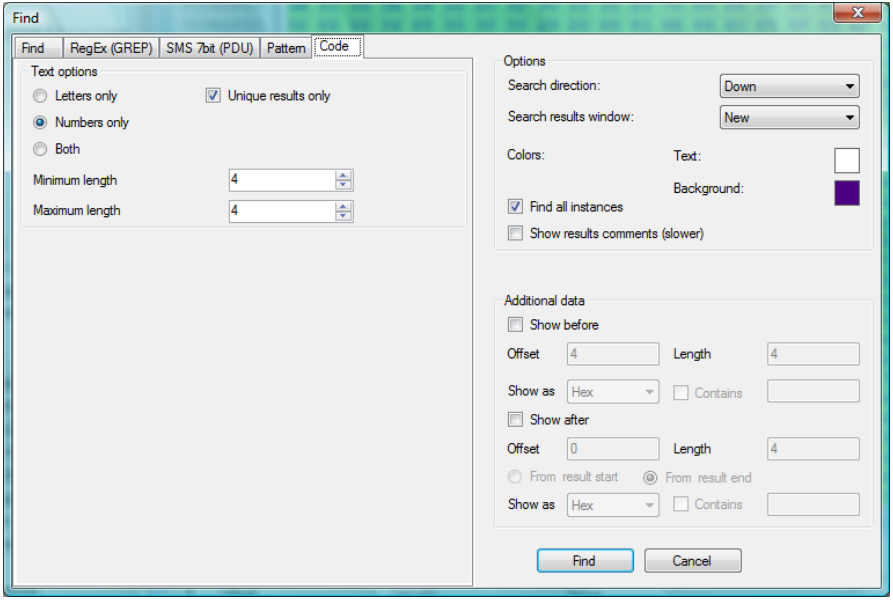
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

10) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
11) To search for specific data and filter the search results, use the **Find** box in the search results tab.
12) To export the search results list, click the desired output in the **Search** tab toolbar: Excel , HTML , PDF , or XML .

12.1.9. Searching for codes and passwords

Search large memory structures for user codes and passwords.

1) While viewing Hex data, click to open the Find window.
2) Select the **Code** tab.



3) In the **Text Options** area, set the following search parameters:
    a) Set the search type: **Letters only**, **Numbers only**, or **Both**.
    b) To show unique results, select **Unique results only**.
4) In the **Minimal length** and **Maximal length** fields, set the pattern length range.

This option enables you to filter the results according to the searched patterns.

5) In the **Options** area, set the desired search options:
   a) In the **Search direction** list, select the search direction.
   b) In the **Search results** window list, select **New**, **Replace current**, or **Add to current**, as desired.
   c) To set the **Text** and **Background** colors, click the color box, select the desired color, and click **OK**.

      The colors you set here are retained for the duration of this session. To change the default colors, set the colors in the Setting window. For more information, see *Hex viewer settings* (page *320*).

      Tip: To easily distinguish between the given results of each search performed, set different text and background colors for each search you run.
   d) Do one of the following:
      - Select **Find all instances** to display all search results at the end of the process
      - Clear **Find all instances** to move through the found items one-by-one during the search (can also be done by pressing F3).
   e) Select **Show results comments** to display
6) In the **Additional data** area, enhance your search capabilities by including a predefined number of characters before and/or after the searched value. This can help you locate specific results, or even limit the results to specific entities of the searched value.

a) Select **Show before** to show the data immediately before what you are searching for.

b) In the **Offset** box, enter the offset from the start of the search result from which to start including the additional data.

c) In the **Length** box, enter the length of the additional data to include starting at the set offset point. For **Show before**, the **Length** cannot be longer than the **Offset**.

d) In the **Show as** box, enter the data type for the additional data to be displayed (**Hex**, **ASCII**, **Unicode**, or **7Bit**).

e) Select **Contains**, and enter a string that the search result must contain in its additional data.

f) Select **Show after** to show the data immediately after what you are searching for, and repeat steps 2-5.

g) For the **Show after** option, set whether the offset and length of the additional data are calculated **From result start** or **From result end**.

The additional data is logged to the **Additional before** and **Additional after** fields of search results.

7) Click **Find**.

If you selected **Find All Instances** in the **Options** area, the results appear in the **Search** results tab in the analysis information tab (in the Hex view tab).

If you did not select **Find All Instances** in the **Options** area, the next found instance is highlighted in the Hex View tab.

The **Search** results tab includes the following:

- **#** - The instance number.
- **Offset** - The address offset of the data file in the Hex data.
- **Length** - The string length in bytes.
- **Value** - The string itself.
- **Source**
- **More**
- **Additional before** - If you set additional data options in the Find window, displays the data located immediately before the result.
- **Additional after** - If you set additional data options in the Find window, displays the data located immediately after the result.

8) To display a result instance in the Hex view tab, click on the desired row in the search results tab.
9) To search for specific data and filter the search results, use the **Find** box in the search results tab.
10) To export the search results list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

12.2. Browsing the hex extraction

- Double-click on a binary hex extraction in the project tree to display its content in a Hex view tab in the data display area.

NOTE: You can also click the image links in the Extraction Log area at the bottom of the Extraction Summary tab to access the Hex extraction.

12.3. Using an offset to jump to a different location in the file

Scan the Hex data by setting an offset value by which to jump through the data.

To move from a set position:

1) Click .
2) Select **Decimal** or **Hex** and in the **Offset** box, enter the offset value in the relevant format.
3) In the **From** area, set the reference point from which to set the offset (**Beginning of file**, **Current position**, or **End of file**).
4) Click **Go**.

   The cursor moves to the offset location.

To move from the current location:

1) Click on a specific location in the Hex data.
2) In the offset value box in the toolbar, enter the desired offset value in decimal format (20) or Hex value format (0x20), or select one of the previously entered values from the list.

NOTE: Type **+** or **-** before the value to calculate the offset from the current position.

3) Do one of the following:
    - Click to jump backwards through the Hex data according to the set value.
    - Click to jump forwards through the Hex data according to the set value.

12.4. Working with bookmarks

A bookmark is a quick reference pointer you can create on Hex data.

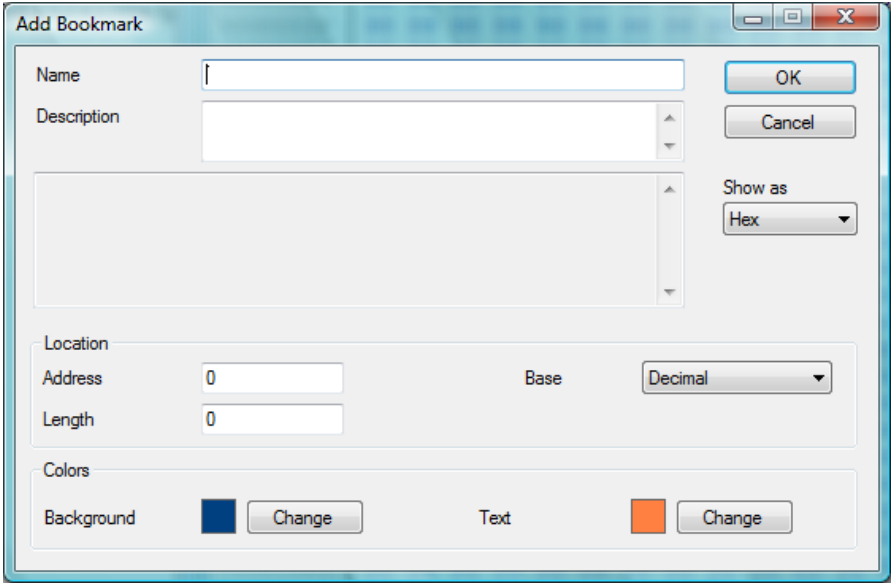
The bookmarks you create are managed in the **Bookmarks** tree item. The number of bookmarks in the project is shown in brackets next to the **Bookmarks** tree item.

- In the project tree, double-click **Bookmarks** to list the bookmarks in a tab in the data display area.
- To print or export the entity bookmarks list, click the desired output in the **Bookmarks** tab toolbar: Excel , HTML , PDF , or XML .

12.4.1. Adding a bookmark

1) While viewing Hex data, do one of the following:
    - In the **Hex View** tab toolbar, click .
    - To bookmark a specific segment in the Hex data, highlight the section that you want to bookmark, and then click in the Hex View tab toolbar.
    - In the **Bookmarks** tab, click .

The Add Bookmark dialog box is displayed.



2) In the **Name** box, enter a name for the bookmark.
3) In the **Description** box, enter a description for the bookmark.

4) If you did not highlight an area in the Hex, in the **Location** area, do the following:
    a) Select the desired unit for the address, **Decimal** or **Hex**, from the **Base** list.
    b) In the **Address** box, enter the address of the start point (offset) of the data you want to bookmark.
    c) In the **Length** box, enter the length of the data you want to bookmark.
5) In the **Colors** area, set the Background and Text colors for the bookmark.
6) Click **OK**.

    The new bookmark is saved and displayed in the Hex view **Bookmarks** tab.

    The marked segment is highlighted in the chosen colors. Details about the bookmark appear in the results window.

    Each bookmark displays the following information:

    - **Offset** - The address offset of the bookmark paragraph in the Hex data
    - **Length** - The bookmarked data segment length
    - **Description** - The bookmark name

7) Click on a bookmark item in the Bookmarks list to display it in the Hex view.

12.4.2. Editing a bookmark

1) In the Hex view **Bookmarks** tab, click .

   The Add Bookmark dialog box is displayed.

2) Change the bookmark as desired, and click **OK**.

12.4.3. Deleting a bookmark

- In the Hex view **Bookmarks** tab, select the bookmark that you want to delete and click .

  The bookmark is deleted.

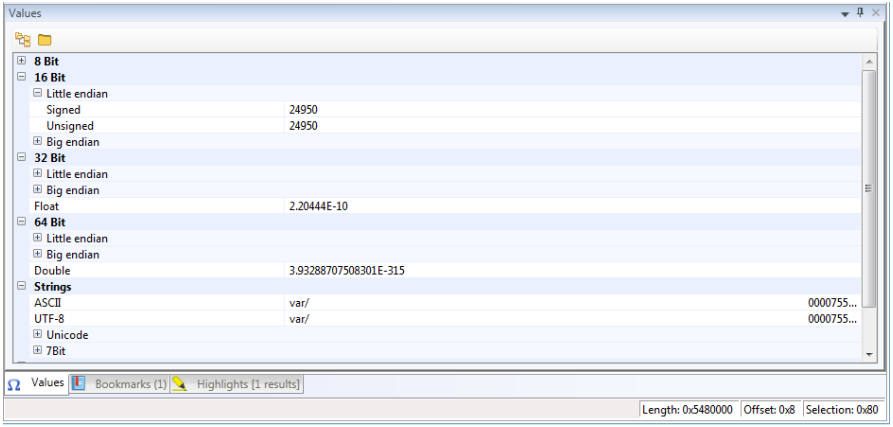
12.5. Decoding raw data

Select segments of the Hex data and decode them to a variety of encoding types on the fly.

UFED Physical Analyzer can decode Hex data to 8 Bit, 16 Bit, 32 Bit, 64 Bit, Strings, Date & Time, Binary, and Numbers.

To decode segments of Hex data:

1) In the **Hex View** tab, select the segment of data that you want to decode.
2) In the **Values** tab at the bottom of the Hex view tab, scroll to the desired encoding, then click to expand the display.



NOTE: Some encoding options have sub-decoding categories.

3) Click or to expand or collapse all the encoding types.
4) To decode a different segment of data, select another segment in the **Hex View** tab.

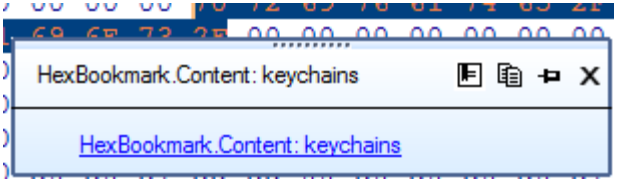
   The results in the **Values** tab change to reflect the selected segment.

12.6. Viewing the hex data information

Display the information of bookmarked segments and search results when you point to them in the **Hex View** tab.

1) In the Hex View tab toolbar, click .
2) Position the mouse over bookmarked information or search results in the Hex.

   The floating information frame appears.



   The following information includes:

   - Links (pointers) to analyzed data items such as files and folders in the project tree.
   - Search results associated with the pointed data.

3) To edit the bookmark, click .
4) To copy the data, click .

   The data is copied to the clipboard.

5) To pin the information frame open, click .

   The information frame remains open and displays the information for the last segment that you point to. The information displayed in the frame is automatically updated when you point to a different bookmarked segment or search result.

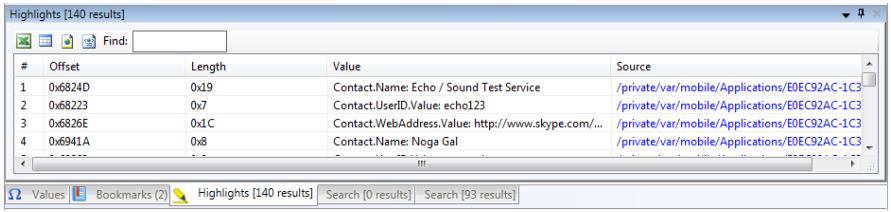
6) To close the information frame, click .

12.7. Locating specific data types in the Hex

The **Highlights** tab presents analyzed data locations within the Hex data, enabling you find the exact location(s) of a particular type of analyzed data in the Hex data.

1) Access the **Highlights** tab at the bottom section of the Hex view.
2) In the project tree, select one of the **Analyzed Data** folders, for example, **Contacts**.

   The selected folder is highlighted in the **Hex View** tab; the **Highlights** tab lists the chunks in the selected folder.


Highlights [140 results]
Find:
Offset Length Value Source
1 0x6824D 0x19 Contact.Name: Echo / Sound Test Service /private/var/mobile/Applications/E0EC92AC-1C3
2 0x68223 0x7 Contact.UserID.Value: echo123 /private/var/mobile/Applications/E0EC92AC-1C3
3 0x6826E 0x1C Contact.WebAddress.Value: http://www.skype.com/... /private/var/mobile/Applications/E0EC92AC-1C3
4 0x6941A 0x8 Contact.Name: Noga Gal /private/var/mobile/Applications/E0EC92AC-1C3
Values
Bookmarks (2)
Highlights [140 results]
Search [0 results]
Search [93 results]

3) To export the Highlights list, click the desired output in the **Search** tab toolbar: Excel, HTML, PDF, or XML.

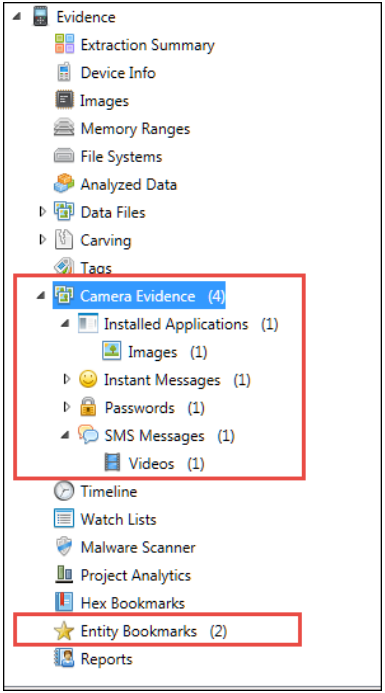
Chapter 13: Camera and screenshot evidence

UFED 4PC or UFED Touch together with the UFED camera enables you to collect evidence by taking pictures or videos of a device. A screenshot feature captures internal screenshots directly from a Blackberry, Android or iOS device. These options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. This evidence can be displayed in UFED Physical Analyzer together with any notes, categories and bookmarks, which were added by the examiner. For information on capturing camera and screenshot evidence, refer to the *UFED 4PC* or *UFED Touch* user manuals.

To import camera or screenshot evidence:

- Click the Evidence.ufd file.

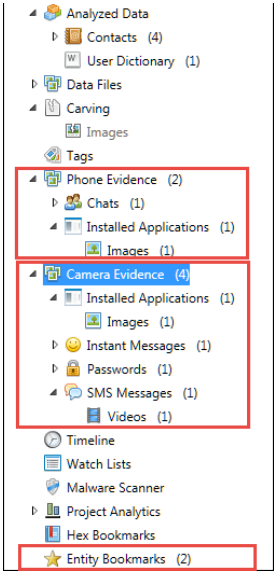
  The Camera Evidence (pictures and videos) or Phone Evidence (screenshots) is imported into UFED Physical Analyzer as a new project. The evidence includes Phone Evidence or Camera Evidence divided by category, as well as entity bookmarks and notes that were added during the extraction. An example is displayed next.


Evidence
Extraction Summary
Device Info
Images
Memory Ranges
File Systems
Analyzed Data
Data Files
Carving
Tags
Camera Evidence (4)
Installed Applications (1)
Images (1)
Instant Messages (1)
Passwords (1)
SMS Messages (1)
Videos (1)
Timeline
Watch Lists
Malware Scanner
Project Analytics
Hex Bookmarks
Entity Bookmarks (2)
Reports

To import camera and screenshot evidence together with the extracted data:

- Click the EvidenceCollection.ufdx file.

  The Camera Evidence (pictures and videos), Phone Evidence (screenshots) and the extracted data are imported into UFED Physical Analyzer as a single project. The evidence includes Phone Evidence and Camera evidence, as well as categories, entity bookmarks and notes that were added during the extraction. An example is displayed next.

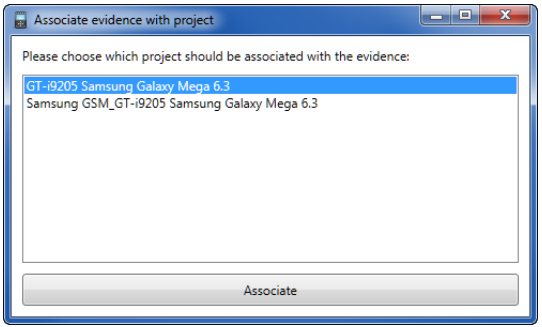


NOTE: Drag-and-drop the EvidenceCollection.ufdx file into UFED Physical Analyzer to open multiple extractions, which were performed for a particular device. That is, all extractions in the folder will be opened. Each extraction (.ufd file) in the folder can also be opened separately. An example folder with multiple extractions and a UFDX file is displayed next.

Name
CaptureScreenshots 2014_08_27 (001) - Samsung GSM Samsung GT-i5510M Galaxy
FileSystemDump Samsung GSM GT-i5510M Galaxy 2014_08_27 (001)
Physical Samsung GSM GT-i5510M Galaxy 2014_08_27 (001)
UFED Samsung GSM GT-i5510M Galaxy 356210042118450 2014_08_27 (001)
EvidenceCollection.ufdx

To associate camera and screenshot evidence with an extraction type:

If you have multiple extraction types as well as camera evidence, the Associate evidence with project screen appears.


Associate evidence with project
Please choose which project should be associated with the evidence:
GT-i9205 Samsung Galaxy Mega 6.3
Samsung GSM_GT-i9205 Samsung Galaxy Mega 6.3
Associate

- Select the required extraction and click **Associate**.

Chapter 14: Advanced decoding

14.1. Managing chains

A chain is a set of plug-ins grouped together, which is used to process the extracted data of a device. Each device in the supported devices list of the application has a predefined parsing chain assigned to it.

As part of its building blocks, a chain can also include other predefined chains.

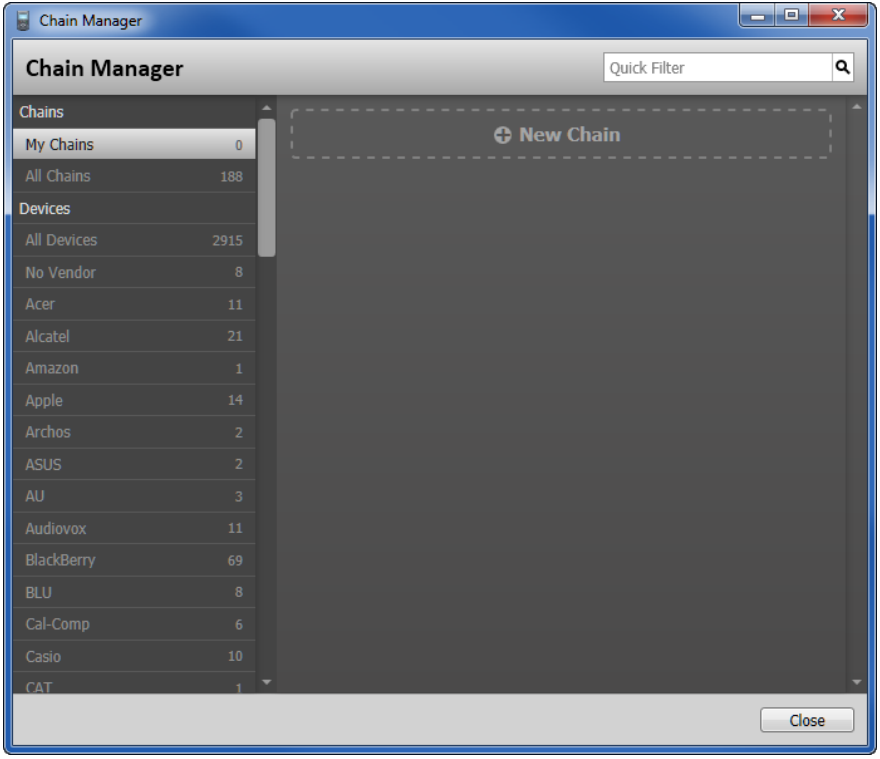
Use the Chain Manager to:

- Manage and edit existing chains
- Create new chains
- Assign chains to devices

To manage application chains:

1) Do one of the following:
    - In the **Plug-ins** menu, select **Chain Manager**.
    - Click .

The Chain Manager window appears.



The **Chains** list on the left enables you to filter the displayed chains list.

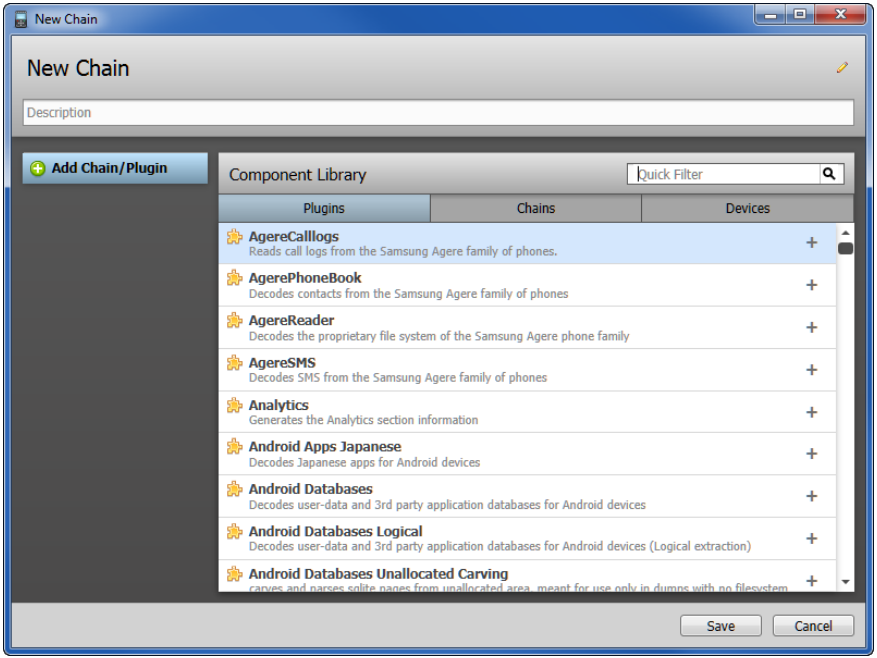
2) Click **My Chains** to display your custom chains.
3) Click **All Chains** to display a list of all the predefined chains.
4) Use the **Quick Filter** box at the top left of the window to filter the displayed list of chains.
5) To display the chains assigned to a specific device, from the Devices section of the list, select one of the following:
    - **All Devices** to display a list of all the predefined devices.
    - A manufacturer name to display a list of the predefined devices of the selected manufacturer.
6) Double click on a device to display its chains window.

   The chains window of the device displays at least one chain that was assigned to it.

14.1.1. Constructing a new chain

1) In the Chain Manager window, click **New Chain**.
2) Click **New Chain**.

The New Chain window appears.



3) Click **New Chain** at the top of the window, and enter a name for the chain.
4) In the **Description** box, enter a short description for the chain (optional).

5) From the Component Library, select a components category:
    - **Plugins** - Specific plug-ins.
    - **Chains** - Specific predefined chains.
    - **Devices** - Entire chain of a specific plug-ins.

   NOTE: **Devices** and **Chains** are added to the chain as a chain component.

6) To add a component to your chain list, click + next to the component.
7) To remove a component from the chain list, click ✖ at the right of the component item, then click **Yes** to approve.
8) To edit the parameters of a plug-in or chain, select it from the chain components list (on the left) and set the options displayed.

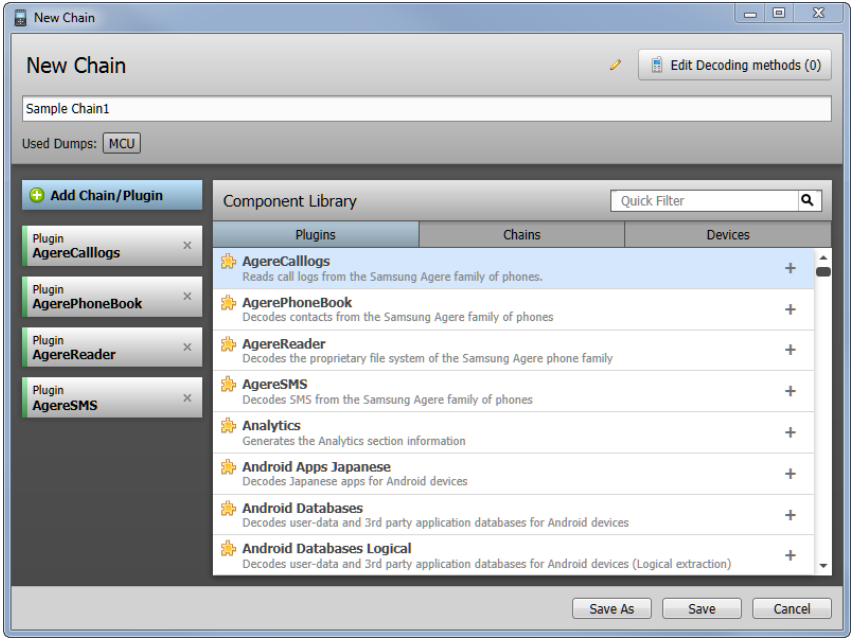
   NOTE: To return to the Component Library display and continue adding more plug-ins and chains, click **Add Chain/Plugin**.

9) When finished, click **Save**.

   The new chain is added to your My Chains list.

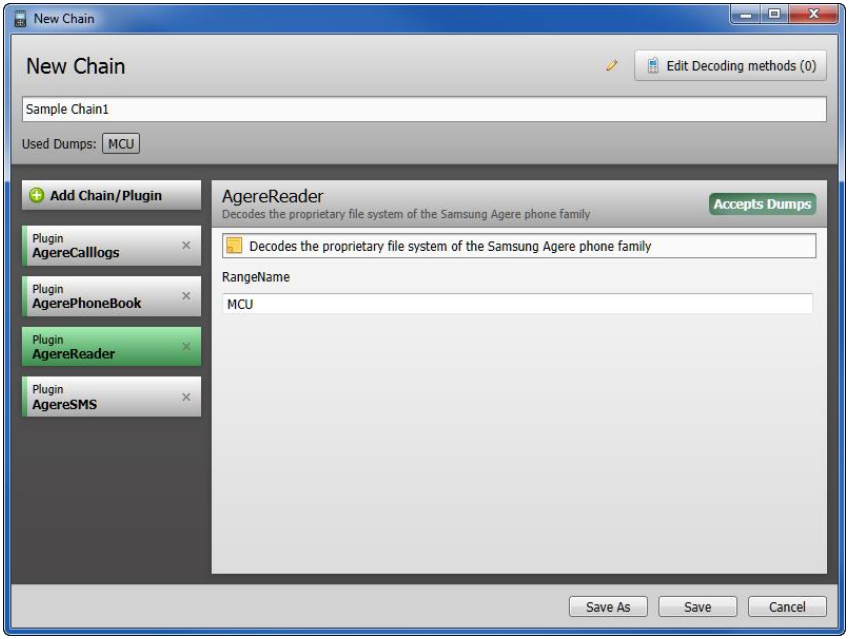
14.1.2. Editing an existing chain

1) Edit chains that you have created.
2) In the Chain Manager **My Chains** list, double-click the chain you wish to edit.
3) Click **Add Chain/Plugin** to display the Component Library.



4) To add a component to your chain list, click + next to the component.
5) To remove a component from the chain list, click ✖ at the right of the component item, then click **Yes** to approve.

6) To edit the parameters of a plug-in or chain, select it from the chain components list (on the left) and set the options displayed.



NOTE: To return to the Component Library display and continue adding more plug-ins and chains, click **Add Chain/Plugin**.

7) When finished, click **Save**, or **Save As** to save the edited chain as a new chain.
8) If you selected **Save As**, enter a name for the new chain and click **Save**.

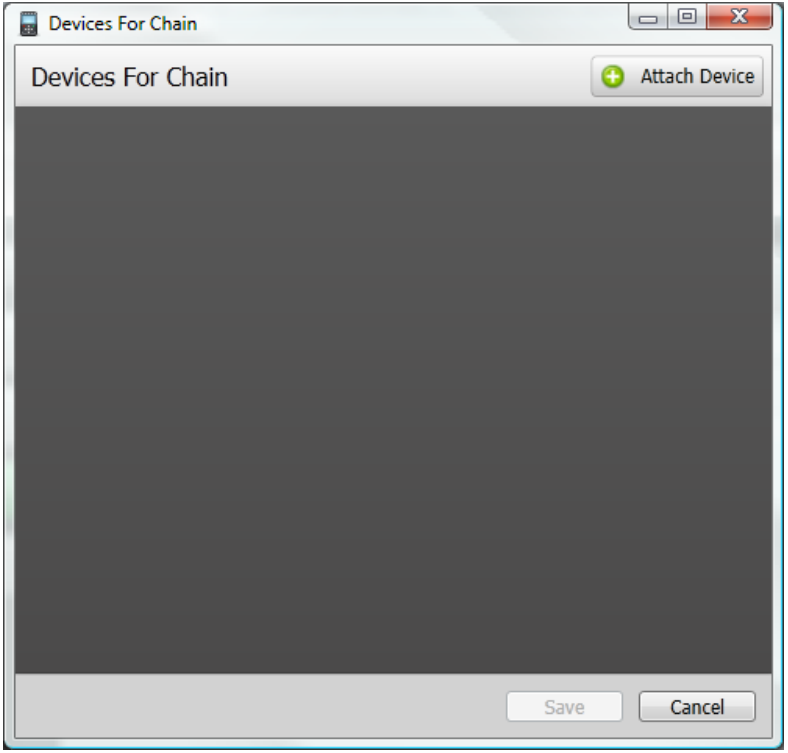
NOTE: Changes made to factory predefined locked chains can only be saved as a new chain

14.1.3. Managing device chains

14.1.3.1. Attaching devices to a chain

You can attach devices to chains you have created, or modify device chains and save them as a copy.

1) Double-click the chain to which you want to attach a device.
2) Click **Edit Devices**.



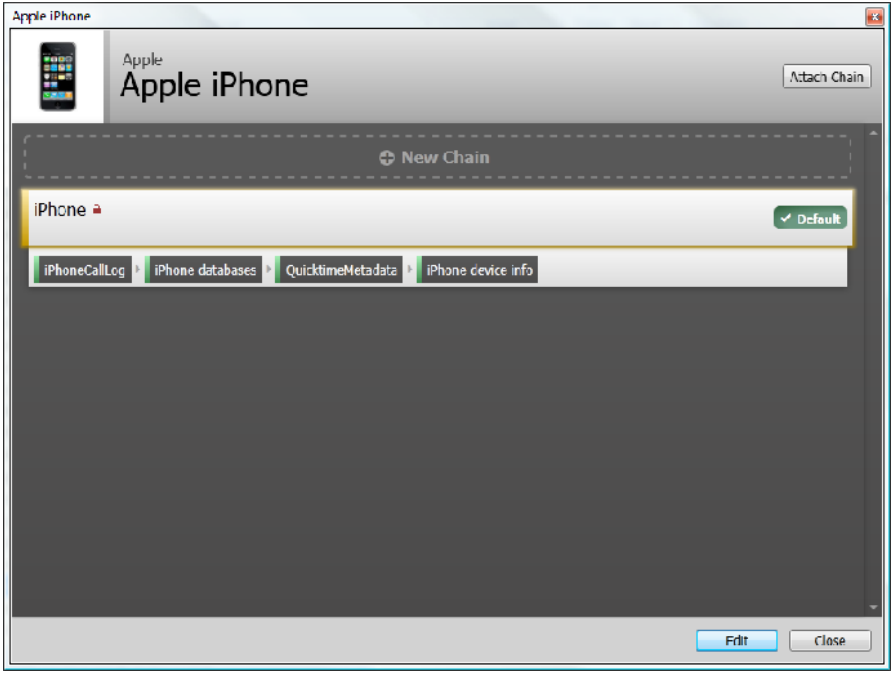
3) In the Devices For Chain window, click **Attach Device**.

4) In The Select Device window, select the device you would like to attach to the chain.

5) Click **Select**.
6) Repeat steps 3-5 to add more devices.
7) When you have finished attaching the devices, click **Save**.

14.1.3.2. Setting the default device chain

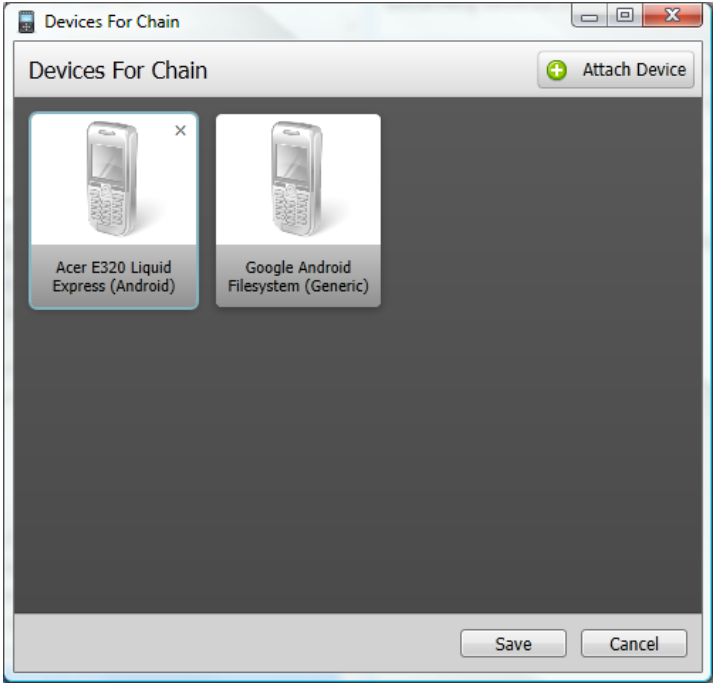
1) In the Chain Manager window, use the Devices list to locate the device you wish to modify.
2) Double-click on the device to display its chains window.



3) If the chains list of the device contains more than one chain, click ✓ to set it as the default chain of the device.
4) Click **Close** to close the device chains window.

14.1.3.3. Detaching devices from a chain

1) Double click on the chain from which you wish to detach a device.
2) Click **Edit Devices** at the top right of the chain window.



3) Click ✖ at the right of every device you wish to detach from the chain.
4) Click **Close**.
5) Click **Cancel** to close the chain window.

14.1.4. Removing a chain

You can remove chains from the My Chains list only.

1) In the Chain Manager window, select **My Chains**.
2) Click ✖ at the right of the chain.

14.1.5. Chain descriptions

The following table lists selected UFED device chains and descriptions.

Chain name	Description
AndroidContent	Decodes content for Android file systems
AndroidContent Japanese	Decodes content for Android file systems and Japanese apps
AndroidFS	Decodes different file systems on Android. This is part of `Motorola Android` or `AndroidDD` chains
AndroidDD	Decodes certain types of Android devices using the metadata from the extraction

Chain name	Description
AndroidDD Japanese	Decodes certain types of Android devices and Japanese apps using the metadata from the extraction.
AndroidiDen	Decodes Motorola iDen with Android operating system physical extractions
Android Logical with Content	Decodes content for Android logical extractions
AndroidMotorolaYaffs	Decodes Motorola Android device (`AndroidDD`) extractions
AndroidMTK NAND	Decodes NAND extractions of MTK Android devices
AndroidNvidia	Decodes Android devices with an Nvidia chipset
AndroidSamsungFAT	Decodes various Samsung Android phones with FAT file systems
BlackBerryIPD	Decodes BlackBerry backup devices using Cellebrite's default chain
BlackBerry Physical	Decoding BlackBerry physical and/or file system extractions
BlackBerryBackup	Decodes BlackBerry backup extractions
CasioC700Content	Decodes models for the Casio c7X1 series
Generic FAT	Decodes FAT (file allocation table) system
iCloudBackup	Decodes data from Apple iCloud backup
iPhone Japanese Content	Decodes content for Japanese iPhones
iPhone Databases Logical	Decodes iPhone content for logical extractions
iPhoneBackupLogical	Decodes data from iPhone backups for logical extractions
iPhoneFS	Decodes iPhone file systems and content
iPhonePhysical	Decodes Physical iPhone extractions
Motorola Android	Decodes Motorola Android devices

Chain name	Description
Nokia FS	Decodes Nokia file systems
Nokia Content	Decodes all Nokia content
Nokia Predef XSR	Decodes non Symbian Nokia BB5 physical extractions
PantechCdm8999Contents	Decodes SMS, MMS and call logs for the Pantech CDM8999 device
QCAndroid	Decodes Qualcomm Android physical extractions
Qualcomm Winmobile	Decodes the flash translation layer of LG Windows mobile and extracts files and SMS from the file system
Report	Decodes reports into UFED Physical Analyzer
Samsung Qualcomm with Content	Decodes file system and content from Samsung Qualcomm devices
Sanyo Qualcomm CDMA Physical	Decodes the flash translation layer file systems and content of Sanyo CDMA devices with a Qualcomm chip
Symbian Physical	Decodes the flash translation layer and a FAT partition using Symbian
WebOS	Decodes file systems for Web operating system devices (Palm)
WindowsPhone7	Decode extractions of Windows Phone 7 devices
AndroidXSR	Decodes Android devices with the XSR flash translation layer
BlackBerry Filesystem Content	Decodes data from BlackBerry file systems
Android Samsung Nexus	Decodes Samsung Nexus devices
AndroidMTK MMC	Decodes MMC extractions of MTK Android devices

Chain name	Description
Samsung Non Android Content	Decodes content of Samsung devices that are not running Android operating systems
Nokia Predef Content	Decodes content of Nokia Predef devices
Samsung MCUv2 - No MMS, Phonebook	Decodes MCUv2 devices excluding MMS and phonebook
Samsung Qualcomm JTAG with Content	Decodes file system and content from JTAG extractions of Samsung Qualcomm devices.
Windows Mobile XSR JTAG	Decodes JTAG extractions of Windows mobile devices with the XSR flash translation layer
SIM Card FS	Decodes content from file system extractions of SIM cards
LG Qualcomm JTAG with Content	Decodes file system and content from JTAG extractions of LG Qualcomm devices
Sanyo Qualcomm JTAG with Content	Decodes content from JTAG extractions of Sanyo CDMA devices with a Qualcomm chip
Samsung Generic JTAG	Decodes the extraction in all supported methods for Samsung devices
HTC Generic JTAG	Decodes the extraction in all supported methods for HTC devices
Samsung Qualcomm with SMS	Decodes file system and SMS from Samsung Qualcomm devices
iPhone Logical with Content	Decodes iPhone logical report extractions

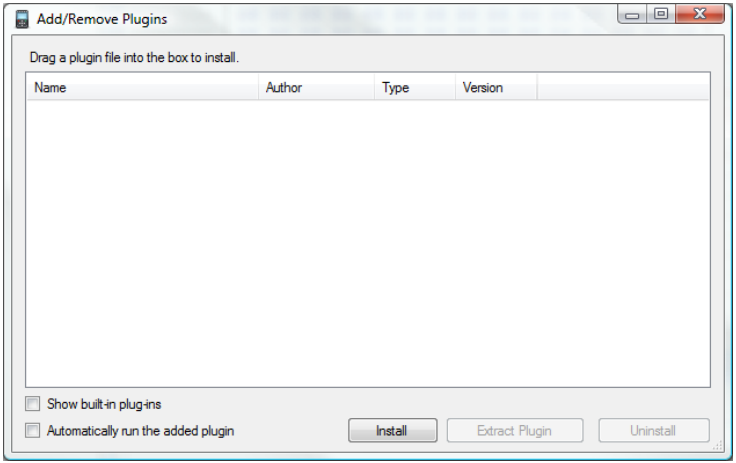
14.2. Plug-ins

The Plug-ins mechanism is an API that allows users to expand the abilities of the application by adding plug-ins provided by Cellebrite, or custom tailored plug-ins written using Python.

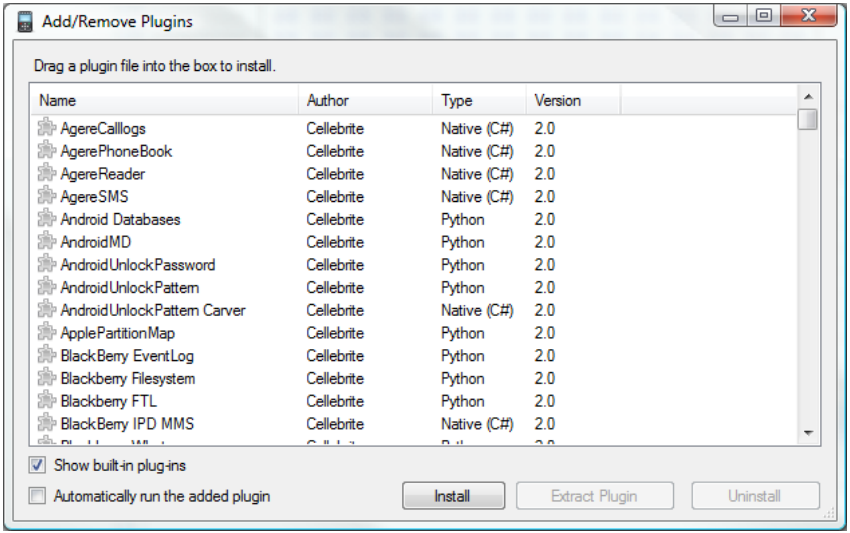
14.2.1. Managing plug-ins

The Add/Remove Plugins window enables you to manage the installed plug-ins.

1) Click .



2) To display all the installed plug-ins, including the built-in plug-ins that cannot be removed, select **Show built-in plug-ins**.



Perform the following tasks in the Add/Remove Plugins window:

3) To install additional plug-ins, drag them to the Add/Remove Plugins window.
4) To extract a copy of an installed plug-in, select the plug-in and click **Extract Plugin**.
5) To remove an installed plug-in, select the plug-in and click **Uninstall**.

NOTE: You cannot extract or uninstall a built-in plug-in of the application.

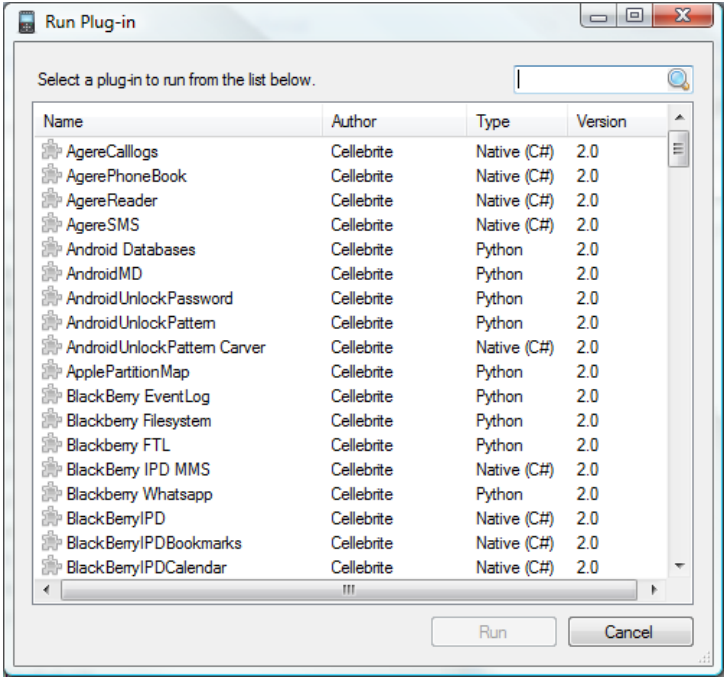
6) To display the plug-in status, double-click the plug-in.

   The Plug-in Status dialog displays the status of the plug-in, which can be either signed or unsigned.

   A signed plug-in is a plug-in that was approved and signed by Cellebrite.

14.2.2. Running a specific plug-in

1) Run an individual plug-in on your project.
2) In the **Plug-ins** menu, select **Run Plug-in**.


Run Plug-in
Select a plug-in to run from the list below.
Name
Author
Type
Version
AgereCalllogs Cellebrite Native (C#) 2.0
AgerePhoneBook Cellebrite Native (C#) 2.0
AgereReader Cellebrite Native (C#) 2.0
AgereSMS Cellebrite Native (C#) 2.0
Android Databases Cellebrite Python 2.0
AndroidMD Cellebrite Python 2.0
AndroidUnlockPassword Cellebrite Python 2.0
AndroidUnlockPattern Cellebrite Python 2.0
AndroidUnlockPattern Carver Cellebrite Native (C#) 2.0
ApplePartitionMap Cellebrite Python 2.0
BlackBerry EventLog Cellebrite Python 2.0
Blackberry Filesystem Cellebrite Python 2.0
Blackberry FTL Cellebrite Python 2.0
BlackBerry IPD MMS Cellebrite Native (C#) 2.0
Blackberry Whatsapp Cellebrite Python 2.0
BlackBerryIPD Cellebrite Native (C#) 2.0
BlackBerryIPDBookmarks Cellebrite Native (C#) 2.0
BlackBerryIPDCalendar Cellebrite Native (C#) 2.0
Run
Cancel

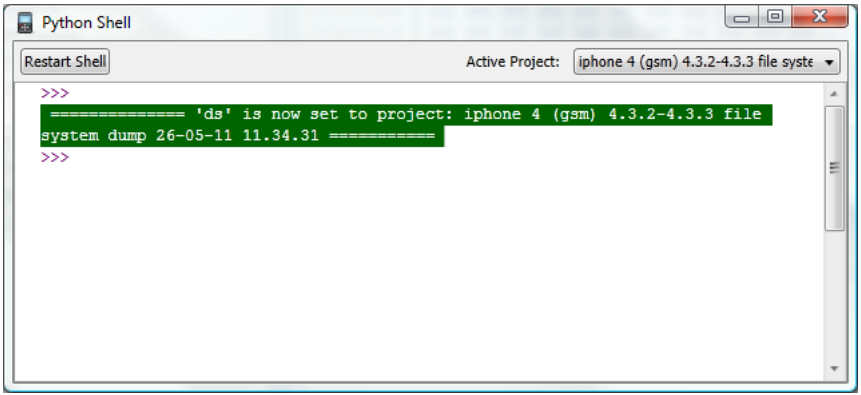
3) Select the desired plug-in from the list of plug-ins, and click **Run**.

14.3. Using the Python Shell

The built-in Python Shell enables you to run customized decoding and analysis using Python commands.

To open the Python Shell window, do one of the following:

1) In the **Python** menu, select **Python Shell**.
2) Click .


Python Shell
Restart Shell
Active Project:
iphone 4 (gsm) 4.3.2-4.3.3 file syste
>>>
========== 'ds' is now set to project: iphone 4 (gsm) 4.3.2-4.3.3 file system dump 26-05-11 11.34.31 ==========
>>>

For additional information on how to use Python Shell commands for custom analysis, refer to the "Python Scripting Guide", accessible from the **Help** menu.

14.4. Exporting the file system

Export the extracted file system to save the entire file system to the selected location on your computer. The save provides the physical files and folders structure saved in the same hierarchy as the original file system.

To export the extracted file system:

1) In the **Tools** menu, select **Dump file system**, or click .
2) In the Browse For Folder dialog, select the target location to which to save the extracted file system.
3) Click **Make New Folder** to create a new folder in the target location.
4) Click **OK** to export the file system.

14.5. Using the Android unlock pattern carver plug-in

Use the Android Unlock Pattern Carver plug-in when working with Android devices where decoding is not yet supported.

The Android Unlock Pattern Carver plug-in can decode unlock patterns on Android devices. The plug-in can be executed on the image file created by the UFED device, JTAG, chip-off, or other tools for which decoding is not yet supported. The image file can be all device partitions, or the user data partition only.

1) Perform physical extraction using the UFED device.

2) In UFED Physical Analyzer, open the Android physical extraction either by dragging and dropping, or by using the "Open Advanced" option.
3) Run the **Android Unlock Pattern Carver** plug-in. For more information on running a plug-in, see *Running a specific plug-in* (page *306*).

   The unlock pattern is presented in the **Extraction Summary** tab **Device Info** area.
4) Unlock the Android device, and perform a physical or file system extraction using the UFED device.

14.6. Android unlock password carver plug-in

UFED Physical Analyzer includes the Android Unlock Password Carver plug-in. The plug-in, developed by the CCL Forensics group and integrated into UFED Physical Analyzer by Cellebrite, attempts to extract the unlock passwords from android extractions. The plug-in can be found in the standard plug-ins list.

Chapter 15: **Settings**

The Settings window provides a set of functional and behavioral setup options used to fine-tune and control the functionality and usability of the application. The settings in the Settings window apply to all the projects open in UFED Physical Analyzer.

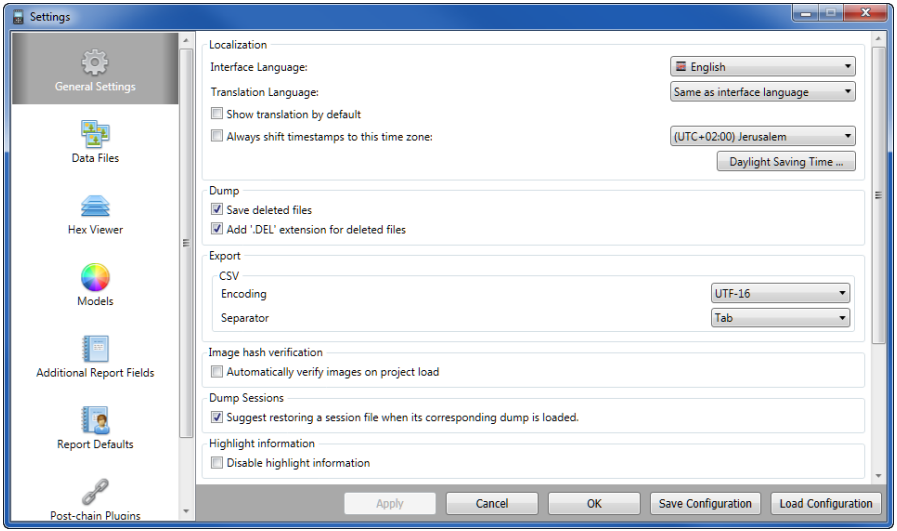
NOTE: Changes to settings are lost when you close UFED Physical Analyzer. To save the settings configuration, see *Saving settings* (page *336*).

- To access the Settings window, do one of the following:
  - Select **Tools** > **Settings.**
  - Click .

  The Settings window appears.

15.1. General settings

Set general application settings in the **General Settings** tab.



To set the interface language of UFED Physical Analyzer:

- In the **Language** list, select the desired language.

To set the translation language:

1) Select the Translation Language. That is the language to which you want to translate the text. You can only select one Translation Language. To request additional translation languages, select **Get more languages**.
2) Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text. To see the translation select **View translated**.

To shift timestamps to a particular time zone:

1) From the Time zone settings (UTC) list, select:
    - Original UTC value to show time stamps as recorded (without unification)
    - One of the time zones (UTC -12:00 to UTC +13:00) to recalculate network-defined time stamps according to the time zone offset.
2) To change the start and end dates for daylight saving time, click **Daylight Saving Time**. For more information on how to change the time zone settings, see *Setting a unified time zone for the project (page 337).*

To set how deleted files are handled when using the Dump GPS / Mass Storage Device feature:

1) In the **Dump** area, select **Save deleted files** to save deleted files.

To set how deleted files are handled when using the Dump GPS / Mass Storage Device feature:

2) In the **Dump** area, select **Save deleted files** to save deleted files.
3) Select **Add '.DEL' extension for deleted files** to save deleted files with the *.DEL extension.

To set the encoding and separator of exported CSV files:

1) In the **Export** area, select the desired encoding option from the **Encoding** list.
2) Select the desired separator in the **Separator** list.

To set UFED Physical Analyzer to automatically verify images on project load:

- Select **Automatically verify images on project load**.

To have UFED Physical Analyzer offer to load a session when opening its corresponding extraction:

- Select **Suggest restoring a session file when its corresponding dump is loaded**.

To disable information highlighting:

- Select **Disable highlight information**.

To select all entities in all views by default:

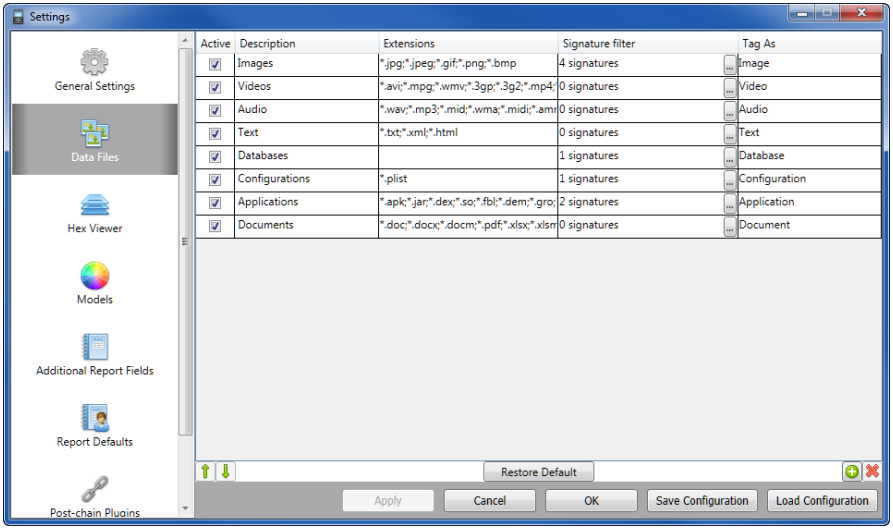
- Select **Check all entities by default**.

  Selected entities are included in reports that you generate.

To determine the number of digits required for phone number uniqueness:

- In the **Analytics** area, select the desired number of digits from the **Number of digits to determine phone number uniqueness**.

15.2. Data files



The **Data Files** settings determine the different file and tagging groups under the **Data Files** and **Tags** tree items, and the types of files filtered in each group.

Every data file record contains the following settings:

- **Active** - Indicates whether to display (checked) or hide (unchecked) this group of data files in the project tree.
- **Description** - A descriptive name for the type of data files to be used as the group name under the **Data files** tree item.
- **Extensions** - The file extensions to be used to filter the data files of this group.
- **Signature filter** - The header and/or footer signatures to be used to filter the data files of this group.
- **Tag As** - The tag name to be applied to the data file and used to list the files under **Tags** in the project tree.

15.2.1. Data files filtering methods

Groups can be filtered using one or more of the following methods:

- Signature filter

  A signature filter is a definition of the file header and/or footer to be searched, in order to detect a file type and associate it with a specific Date File group. The header and/or footer can be configured in a defined range from the beginning and end of the file respectively by using the offset parameter.

For example, a JPEG image starts with the header FF D8 FF and ends with the footer FF D9. Entering this information in the Header and Footer fields of the signature creates a signature that identifies JPEG images.

- Extension filter

  An extension filter is a list of common file extensions that are associated with file formats that belong to the specific data file group.

  For example, the different image file formats can be filtered by the file extensions *.jpg, *.jpeg, *.gif, *.png or *.bmp.

15.2.2. Managing data files settings

Add new types of data files, and edit and delete existing data file types.

15.2.2.1. Adding a new data file type

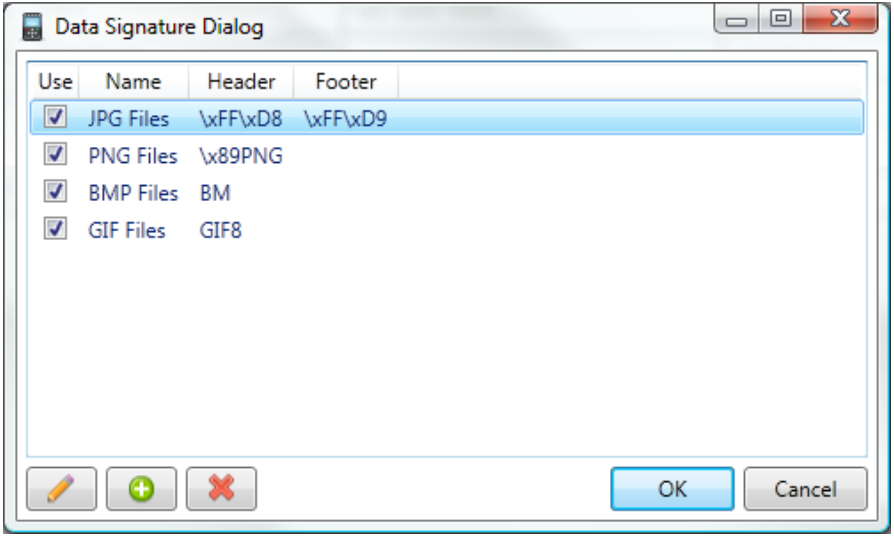
1) In the **Data Files** settings, click .

   A new row is added to the list.

2) Select **Active** to display the added data type in the **Data Type** tree item.
3) Click in the new row's **Description** box, and type a file type description.

4) If applicable, in the **Extensions** box, enter the file extensions commonly used by your data file type in the format ***.xxx**, and separated by ;.

5) If applicable, in the **Signature filter** box, click and do any of the following:



- Click to add a filtering signature that identifies your data file type.
- Click to edit an existing signature filter.

- Click to delete a signature filter.

6) If applicable, click in the **Tag As** box, click and select a tag name from the list.
7) To change the order of the data file types, use the arrows .
8) To clear the list of data file types you added, leaving only the default types, click **Restore default**.

15.2.2.2. Editing an existing data file record

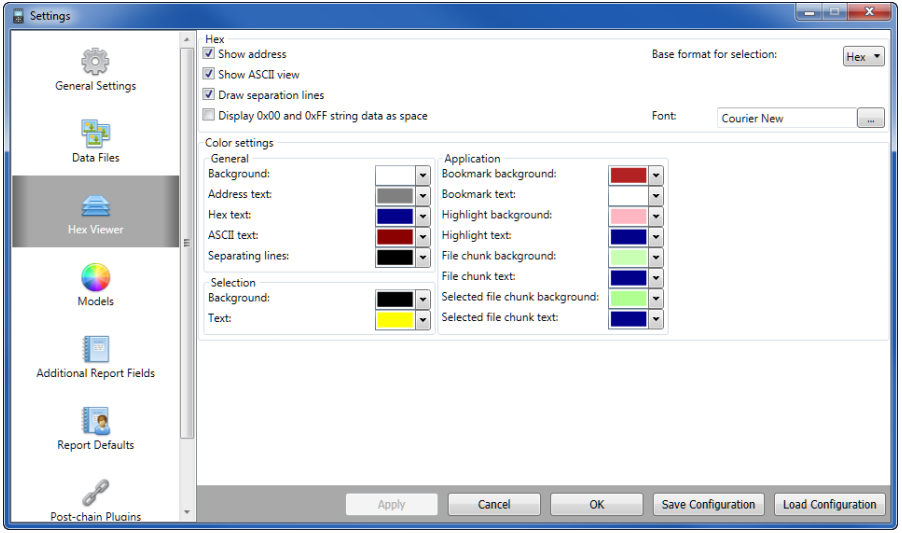
1) Click the row of the data file type that you want to edit.
2) Double-click in the column and row that you want to change, and update the existing settings as desired.

15.2.2.3. Deleting a data file type

1) Click the row of the data file type that you want to delete.
2) Click .

15.3. Hex viewer settings

The Hex Viewer setting enables you to control the display options of Hex extractions to suit personal preference and enhance readability.

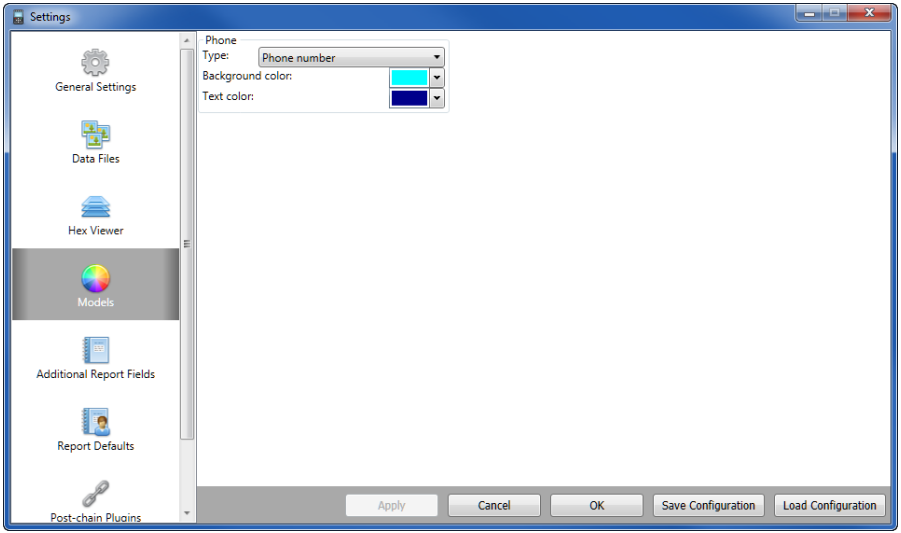


Change the defaults for the following Hex viewer settings:

- **Show address** - Show/Hide the line numbers column of the Hex Viewer.
- **Show ASCII view** - Show/Hide the ASCII view column of the Hex Viewer.
- **Draw separation lines** - Show/Hide the separation lines between the address, Hex data, and ASCII view columns
- **Display 0x00 and 0xFF string data as space** - Set the string data to display both 0x00 and 0xFF characters as space instead of a ".".
- **Base format for selection** - The line numbers format (Decimal, Hex, or Both).
- **Font** - The font used to display the information.
- **Color settings** - Set the colors applied to different features of the Hex viewer.

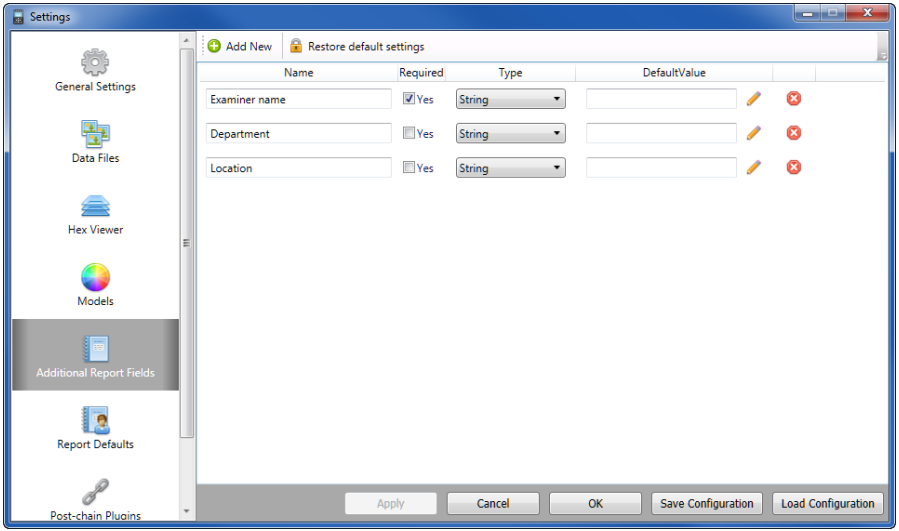
15.4. Models settings

Set the color schemes to be applied to various types of device data.



1) In the **Type** list, select the data type.
2) In the **Background color** list, select the desired background color.
3) In the **Text color** list, select the desired background color.

15.5. Additional report fields



Optional information is user-defined information presented at the beginning of the report. It usually includes information about the case, investigator, and organization details.

Every optional information record consists of the following:

Name	The name of the report field.
Required	Indicates if the field must be filled in order to generate the report
Type	The types of entry - **String** or **List**.
Default value	Default content.

You can add new report fields, and edit and delete fields, as desired.

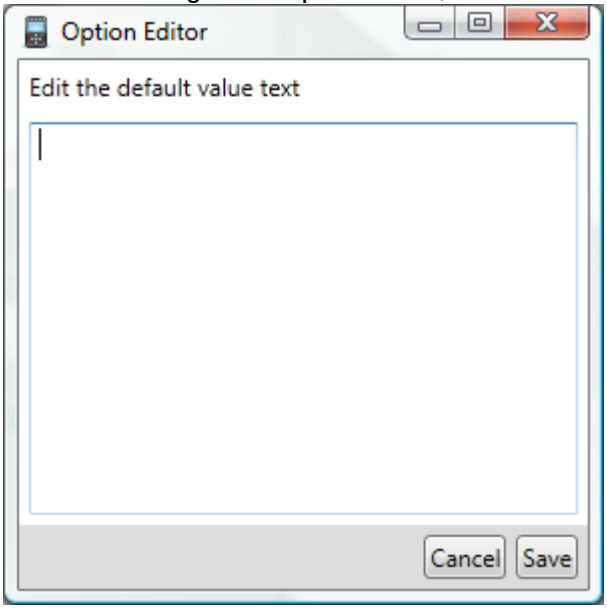
15.5.1. Adding a new report field

1) Click **Add New.**

   A new row is added to the table.

2) In the **Name** column, enter the name label to be displayed.
3) Select **Required** if this field must be filled in order for the user to generate the report.
4) In the **Type** list, select one of the following:
   - **String** for text entry fields
   - **List** for a specified list of options
5) In the **Default Value** box, set the default content:

- For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, then click **Save**.



- For a **List** type, click , enter the list items with each item on a separate line, then click **Save**.

15.5.2. Editing a report field

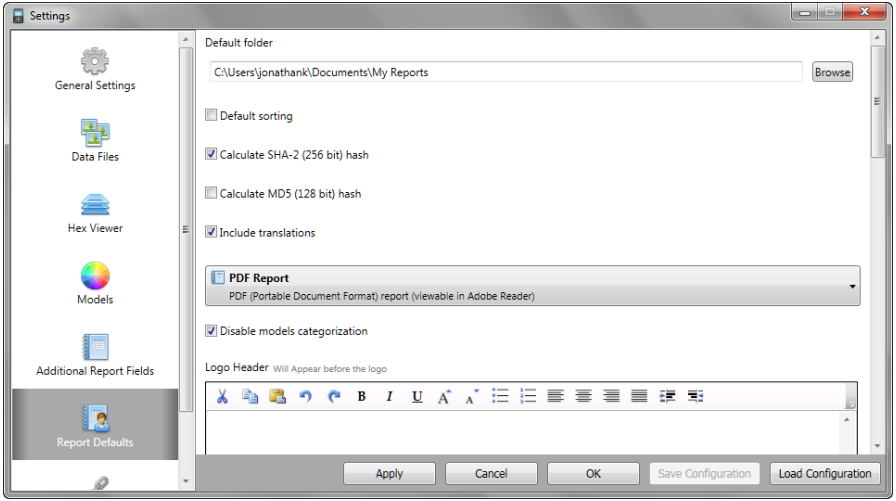
- To edit a report field, perform steps 2-5 of *Adding a new report field* (page *324*), changing the parameters to suit your needs.

15.5.3. Deleting a report field

- To delete a report field, click .

15.6. Report defaults

The **Report Defaults** settings enable you to edit the report presentation.



NOTE: Scroll down to see all the fields.

1) In the **Report type** list, select the report type that you want to edit.
2) For Excel reports, set the following:
    - **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
    - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting

order (ascending or descending) that was set by the user in each of the data display tables.

- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Unprintable characters placeholder** - Set the placeholder character to replace the unprintable characters.
- **Output File Format** - Set the output file format of the spreadsheet file to either:

* **XLSX** - The current Excel file format.

* **XLS** - The legacy file format of Excel.

* **ODS** - The spread file format of OpenOffice.

- **The excel report is compatible with OpenOffice** - Select to ensure the Excel report can be opened in OpenOffice.
- **Generate Contact Identification Data** - Select to add a sheet to the Excel report that provides a list of unique contacts based on type.

3) For HTML reports, set the following:

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting

order (ascending or descending) that was set by the user in each of the data display tables.

- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Disable models categorization** - Select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.

- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.
- **Split HTML report** - Set each section of the report to start on a new page.

4) For PDF reports, set the following:

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.

- **Disable models categorization** - select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.

- **Display all chat messages** - Display all chat messages in the report.

5) For UFED report packages, set the following:
   - **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
   - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
   - **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
   - **Include translations** – Select to include any translated text in the report.
6) For Word reports, set the following:
   - **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
   - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.

- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Disable models categorization** - Select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.

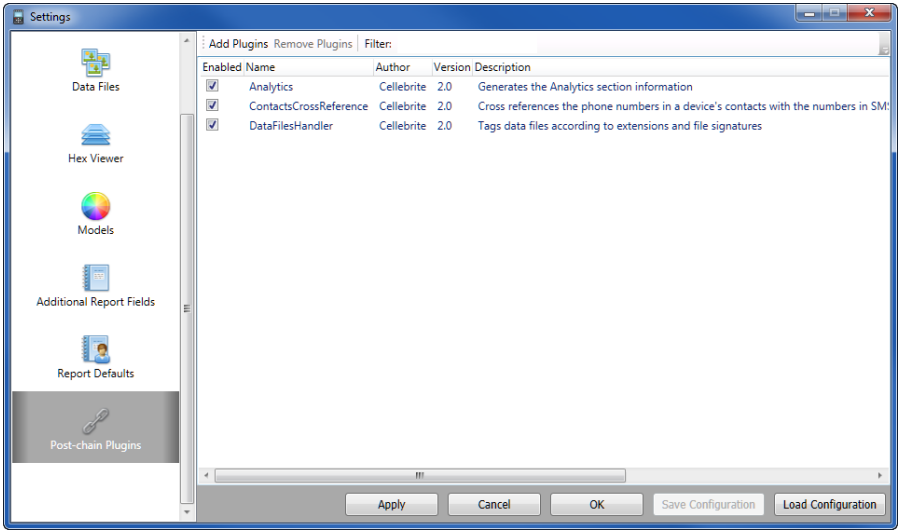
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report. The report includes links to text files containing the entire email.
- **Display full email body** - Set to display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.

7) For XML reports, set the following:

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.

15.7. Post-chain plugin settings

Add and remove plug-ins from the list of plug-ins that automatically run when you open a project. This can be useful when you have time constraints or large extraction files. These settings enable you to define whether or not to run certain plug-ins.



1) To add a plug-in to the list, click **Add Plugins** and select a plug-in from the list.
2) To remove a plug-in from the list of plug-ins that run automatically when you open a project, clear the check box in the **Enabled** column.
3) To remove a plug-in from the list, select the plug-in and click **Remove Plugins**.
4) To filter the plug-ins list, use the **Filter** box.

NOTE: The settings apply to subsequent projects opened in your current session. To save your configuration settings for use in subsequent sessions, see *Saving settings* (page *336*).

15.8. Saving settings

Save your settings to reuse later, or to share with another user.

1) In the Settings window, click **Save Configuration**.
2) In the Save As window, browse to the location where you want to save your settings configuration, and click **Save**.

   The settings are saved as a UFED Physical Analyzer Settings Configuration File (*.cnf).

15.9. Loading settings

Load your saved settings configuration.

1) In the Settings window, click **Load Configuration**.
2) In the Open window, browse to the location where your settings configuration is saved, select the configuration (*.cnf), and click **Open**.

   The settings are applied in the Settings window.

15.10. Setting project settings

Set unified time zone and case information for each project.

15.10.1. Setting a unified time zone for the project

During extraction, one time stamp per event is extracted.

For outgoing events, the time stamp is typically taken from one of the following sources:

- User-defined device time (where the device time has been manually set by the user: timestamps are displayed without the unified time (UTC).
- Network-defined device time (where the device time is automatically set by the network): timestamps are displayed with the unified time (UTC).

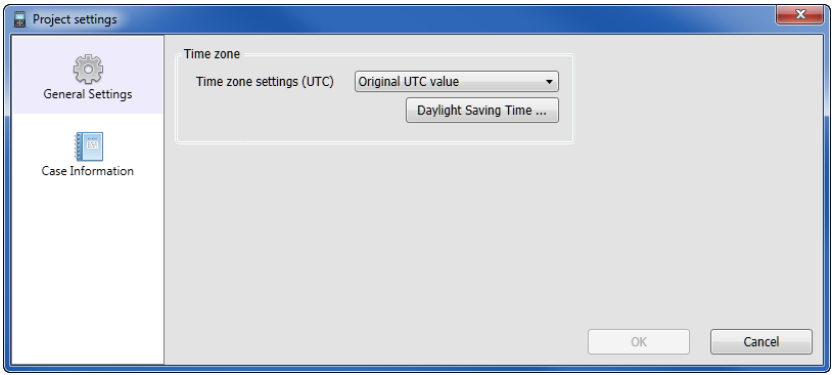
For incoming events, the time stamp is typically taken from the network-defined time (the time stamp assigned by the network); timestamps are displayed with the unified time (UTC).

Network-defined time stamps are subject to the time zones in which the event occurred.

Apply a unified time zone to the project to recalculate all network-defined time stamps according to the selected time zone in order to consolidate the events and view them sequentially in UFED Physical Analyzer.

To apply a unified time zone to the project:

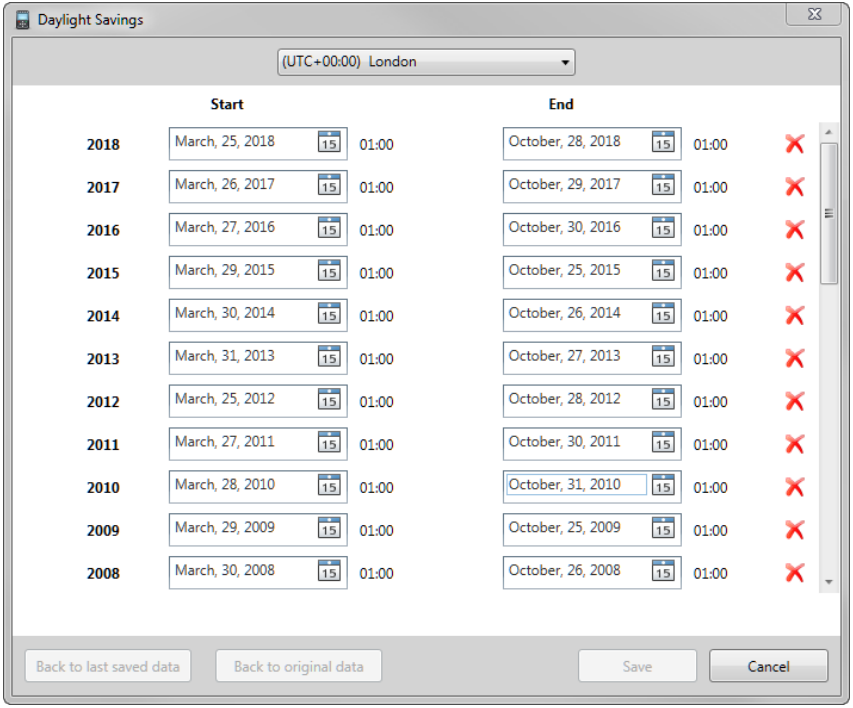
1) Do one of the following:
   - In the project **Extraction Summary** tab, click **Project settings**.
   - Click .



2) From the **Time zone settings (UTC)** list, select:
   - **Original UTC value** to show time stamps as recorded (without unification)
   - One of the time zones (**UTC -12:00** to **UTC +13:00**) to recalculate network-defined time stamps according to the time zone offset.

   NOTE: User-defined time stamps are not included in these recalculations, and are displayed as recorded.

3) To change the start and end dates for daylight saving time, click **Daylight Saving Time**.


Daylight Savings
(UTC+00:00) London
Start
End
2018 March, 25, 2018 01:00 October, 28, 2018 01:00
2017 March, 26, 2017 01:00 October, 29, 2017 01:00
2016 March, 27, 2016 01:00 October, 30, 2016 01:00
2015 March, 29, 2015 01:00 October, 25, 2015 01:00
2014 March, 30, 2014 01:00 October, 26, 2014 01:00
2013 March, 31, 2013 01:00 October, 27, 2013 01:00
2012 March, 25, 2012 01:00 October, 28, 2012 01:00
2011 March, 27, 2011 01:00 October, 30, 2011 01:00
2010 March, 28, 2010 01:00 October, 31, 2010 01:00
2009 March, 29, 2009 01:00 October, 25, 2009 01:00
2008 March, 30, 2008 01:00 October, 26, 2008 01:00
Back to last saved data
Back to original data
Save
Cancel

a) For the year that you want to change, use the calendar to select the start and end dates, or edit the dates directly. You can use the button to remove certain years.

b) Click **Back to last saved data** to reset the table to the last time that you saved the data, click **Back to original data** to return the table to its default settings, or click **Save** to save the table with any changes that you made.

4) Click **OK**.

The project is recalculated according to the selected unified time zone, and the new time zone is applied to the network-defined time stamps. Time stamps of events displayed in UFED Physical Analyzer windows and any subsequently-generated reports reflect the selected unified time zone.

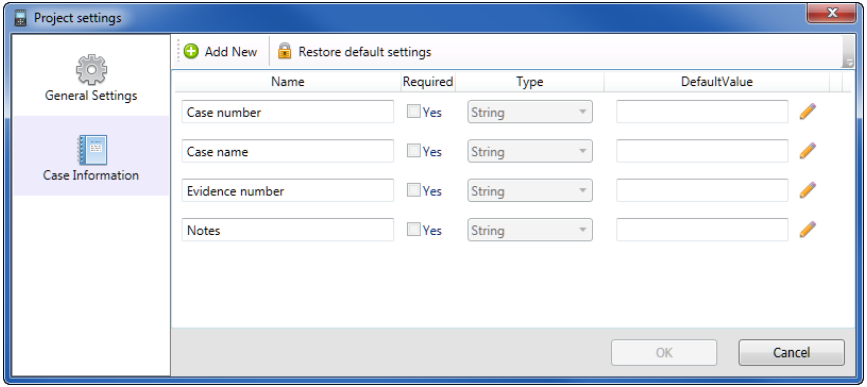
15.10.2. Setting the case information

Case information settings are saved with the project. The case number appears with the extraction information on the Welcome tab.

1) Do one of the following:

- In the project **Extraction Summary** tab, click **Project settings**.
- Click .

2) Click **Case Information**.



3) Click **Add New**.

   Some case information fields appear by default.

4) Set the parameters for the default information fields:

   a) In the **Name** column, enter the relevant information (for example, case number, name, or notes).

   b) Select **Required** if this field must be filled.

   c) In the **Type** list, select one of the following:

   - **String** for text entry fields
   - **List** for a specified list of options

d) In the **Default Value** box, set the default content:

- For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, then click **OK**.
- For a **List** type, click , enter the list items with each item on a separate line, then click **OK**.

5) To add more information fields, click **Add New**, and repeat step 3.
6) To remove the custom entries, click .
7) To restore the default settings, click **Restore default settings**.

Chapter 16: Reference

16.1. File menu

Open	Open a file for analysis using the standard analysis process.
Open (Advanced)	Open a file for analysis using the advanced analysis process. See *Opening an extraction in advanced mode* (page *41*).
Recent	Displays a list of recent projects.
Close	Closes the currently active project
Save Project Session	Saves the active project information generated by the user as a Physical Analyzer Session File (*.pas). See *Saving a project session* (page *65*).
Load Project Session	Loads a Physical Analyzer Session File (*.pas) onto an open project in the project tree.
Exit	Closes the UFED Physical Analyzer and all active sessions.

16.2. View menu

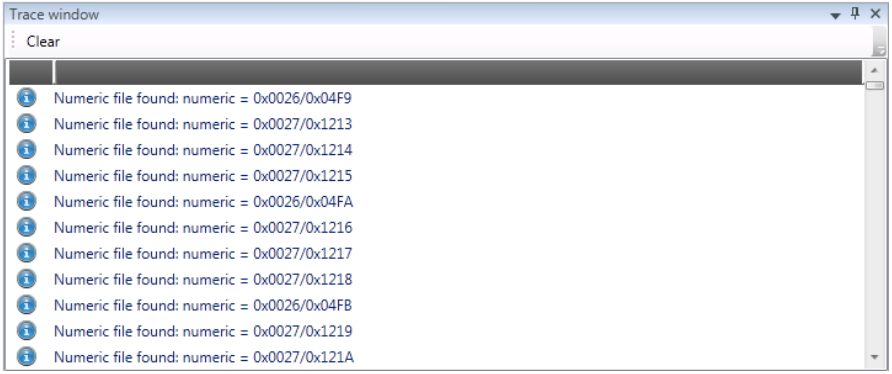
Show Welcome Screen	Displays the **Welcome** tab. See *Welcome tab* (page *85*).
Trace Window	Show/hide the trace panel at the bottom of the data display area.

16.2.1. Viewing the trace window

Show the Trace window at the bottom of the data display area to view a log of the actions performed in your session by you or by UFED Physical Analyzer, such as plug-in activation.

1) In the **View** menu, select **Trace Window**.

   The Trace window appears below the data display area.


Trace window
Clear
Numeric file found: numeric = 0x0026/0x04F9
Numeric file found: numeric = 0x0027/0x1213
Numeric file found: numeric = 0x0027/0x1214
Numeric file found: numeric = 0x0027/0x1215
Numeric file found: numeric = 0x0026/0x04FA
Numeric file found: numeric = 0x0027/0x1216
Numeric file found: numeric = 0x0027/0x1217
Numeric file found: numeric = 0x0027/0x1218
Numeric file found: numeric = 0x0026/0x04FB
Numeric file found: numeric = 0x0027/0x1219
Numeric file found: numeric = 0x0027/0x121A

2) To clear the log, in the Trace window, click **Clear**.
3) To close the Trace window, click .

The Trace window can be hidden or displayed.

- To pin the Trace window open, click .
- To unpin the Trace window, click .
- To view the Trace window when hidden, select or mouse over the tab.

16.3. Tools menu

Read Data from UFED	Enables data extraction directly to the computer.
Dump File System	Exports and saves the parsed file system to actual files and folders in a directory structure. See *Exporting the file system* (page *309*).
Carve Images	Opens the Carve Images window from where you can scan for images. See *Carving images* (page *220*).
Carve Strings	Opens the Carve Strings window from where you can scan for strings.
Watch List Editor	Opens the Watch List Editor, from where you can create, manage, and run your watch lists. See *Working with watch lists* (page *122*).
Malware Scanner	Opens the Malware Scanner sub-menu, from where you can run malware detection on your extraction, and update the signature database. See *Scanning for malware* (page *163*).
Translation	Downloads the translation pack from the Internet, installs the translation pack from a file, or displays the supported languages. See *Translating decoded data* (page*147*).
Open in UFED Link Analysis	Open this Physical Analyzer project in UFED Link Analysis.
TomTom	Opens the TomTom sub-menu, from where you can export the TomTom extraction file and import the returned xml file. See *Working with TomTom* (page *217*).
Settings	Access the application settings window. See *Settings* (page *311*).

Project Settings	Set unified time zone and case information for each project. See *Setting project settings* (page *337*).

16.4. Extract menu

iOS Device Extraction	Starts iOS Device Extraction to perform extractions from iOS devices. See *Extraction from iOS devices* (page *183*).
Extract GPS/Mass Storage Device	Reads and saves data from GPS and mass storage devices connected to the workstation via USB connection. See *Reading data from a GPS or mass storage device* (page *213)*.

16.5. Python menu

Python Shell	Opens the Python Shell window for user customer analysis using Python commands. See *Using the Python Shell* (page *308)*. For additional information on how to use Python Shell commands for custom analysis, refer to the "Python Scripting Guide", accessible from the **Help** menu.
Run Script	Runs a pre-written Python script (*.py file).
Run Script (Debug enabled)	Enables you to run a pre-written Python script (*.py file) in debug mode.

16.6. Plug-ins menu

Add/Remove Plug-ins	Displays the list of pre-installed plug-ins to enable management of the currently installed plug-ins. See *Managing plug-ins* (page *304*).
Run Plug-in	Enables the user to select a specific plug-in and run it. See *Running a specific plug-in* (page *306*).
Chain Manager	Displays the Chain Manager window to enable management and creation of device processing chains. See *Managing chains* (page *287*).

16.7. Report menu

Generate Report	Generates a report summary of all information found by the analysis process. See Generating a report.

16.8. Help menu

Supported Apps	Lists the supported applications and verified versions for Android and iOS devices.
Manual	Opens the user manual in PDF format.
Python Shell Scripting Guide	Opens the Python Scripting Guide in PDF format.
Activate Online Bing Maps	Activates Bing maps so that you can view locations on a map. It requires Internet access and a valid UFED Physical Analyzer license.
Start UFED Link Analysis Demo	Starts the UFED Link Analysis application.
Show License Details	Displays the current software or hardware (dongle) license information, and enables you to: • Activate or load a new license (software or dongle) • Display information about previous dongles that were connected to this workstation • Deactivate a software license • Get direct access via email to Cellebrite support and sales
Zip Log Files	Zips the log files and opens the folder where the zipped log files are saved.

Zip Log Files with System Information	Zips the log files and includes detailed information about the operating system, drivers, application data, event logs etc. This information can be used to analyze report cases.
About	Provides information about the installed UFED Physical Analyzer version.

A

About location data • 75, 137, 217

Activating UFED Physical Analyzer • 25

Activation using a software license • 33, 34

Adding a binary dump • 51, 56, 58

Adding a bookmark • 276

Adding a file system dump • 52, 56, 58

Adding a new data file type • 317

Adding a new report field • 324, 326

Additional report fields • 176, 323

Advanced decoding • 45, 287

Advanced features • 217

Advanced opening of a non-UFED extraction file • 52

Advanced opening of a UFED extraction file • 41

Android Unlock Password Carver plug-in • 310

Attaching devices to a chain • 294

B

Bookmarking information (entity bookmarks) • 80, 134

Browsing the file system • 116

Browsing the Hex extraction • 274

C

Carving images • 77, 220, 348

Changing the decoding chain • 45

Closing a project • 67

Closing UFED Physical Analyzer • 67

Constructing a new chain • 289

Conversation view • 120

Creating a new entity bookmark • 135

Creating a watch list • 123, 132, 133

D

Data analysis • 12

Data display area • 83

Data files • 88, 315

Data files filtering methods • 316

Data tabs • 89

Database view • 98

Daylight saving time • 313

Deactivating version 2 licenses • 33

Deactivating version 5 licenses • 33

Decoding raw data • 279

Deleting a bookmark • 279

Deleting a data file type • 319

Deleting a report field • 326

Deleting a watch list • 131

Deleting an entity bookmark • 137

Detaching devices from a chain • 299

Device Locations • 137

Dongle • 26

E

Editing a bookmark • 279

Editing a report field • 326

Editing a watch list • 127

Editing an entity bookmark • 136

Editing an existing chain • 291

Editing an existing data file record • 319

Editing the current chain • 47, 56, 57

Enabling connectivity with Windows Vista • 17, 35

Exporting a TomTom file • 218

Exporting a watch list • 130

Exporting the file system • 309, 348

Extract menu • 349

Extracting data from a device with a complex password • 197

Extracting data from a device with a simple password • 195

Extraction from GPS or mass storage devices • 210

Extraction from iOS devices • 183, 349

Extraction summary tab • 87

F

File Info tab • 107

File menu • 345

Folder view • 97

G

General settings • 312

Generating a Report - Report Wizard • 173

Getting started • 37

H

Help menu • 351

Hex view • 100, 117, 229

Hex viewer settings • 234, 239, 243, 248, 253, 257, 262, 267, 272, 320

I

Image capture • 283

Importing a TomTom file • 219

Importing a watch list • 128

Installation and Activation • 15

Installing UFED Physical Analyzer • 16, 18

Introduction • 9

J

JTAG • 58

L

Launching UFED Physical Analyzer • 37

Legal notices • 3

Link Analysis Demo • 38

Loading a project session • 66

Loading settings • 337

Locating a watch list • 134

Locating and analyzing information • 111

Locating specific data types in the Hex • 282

M

Managing chains • 50, 287, 350

Managing data files settings • 75, 317

Managing device chains • 294

Managing plug-ins • 304, 350

Markers and information windows • 143

Models settings • 322

Moving UFED Physical Analyzer with a software license to another PC • 32

N

Network dongle • 30

New version notification • 25

O

Obtaining a copy of UFED Physical Analyzer • 17

Opening an extraction for analysis • 38

Opening an extraction in advanced mode • 38, 40, 41, 345

Orientation to the workspace • 37, 69

Overview • 9

P

Performing advanced logical extraction • 199

Performing extractions • 183

Performing physical extraction • 184

Performing physical extraction from encrypted devices • 193, 194

Performing physical extraction from non-encrypted iOS devices • 185, 195, 197

Physical extraction • 10

Playing video or audio files • 110

Plug-ins • 45, 304

Plug-ins menu • 350

Post-chain plugin settings • 335

Prerequisites • 183

Project tree • 70, 88, 134

Python menu • 349

R

Reading data from a GPS or mass storage device • 213, 217, 349

Reference • 345

Removing a chain • 300

Report defaults • 176, 326

Report menu • 350

Retrieving addresses • 144

Running a specific plug-in • 306, 310, 350

Running a watch list • 132

Running a watch list on particular projects • 132

Running a watch list on your current project • 133

S

Saving a .ufd file • 64

Saving a customized chain • 50

Saving a project session • 65, 345

Saving settings • 66, 311, 336

Scanning for carved images • 221

Scanning for malware • 81, 163, 348

screenshots • 283

Searching bytes • 231, 237

Searching dates • 231, 241

Searching for codes and passwords • 232, 270

Searching for information in a data tab • 111

Searching for information in all open projects • 115

Searching for information in the Hex data and decoded data • 230

Searching for patterns • 232, 265

Searching for regular expressions (GREP) • 231, 255

Searching SIM ICCID numbers • 231, 246

Searching SMS numbers • 231, 251

Searching SMS text strings • 232, 260

Searching strings • 231, 232

Selecting a different chain • 46, 56, 57

Selecting languages • 148

Setting a unified time zone for the project • 337

Setting project settings • 82, 337, 349

Setting the case information • 176, 341

Setting the default device chain • 297

Settings • 311, 348

Shortcuts • 68

Software installation • 17

Software license • 28

Specifying a different device • 44, 56, 57

Starting from a blank project • 54, 56

Starting with device selection • 54

System requirements • 16

T

Table view for analyzed data • 96

Table view for data files • 94

Text view • 93

Time line view • 117

Tools menu • 348

Translating decoded data • 147

U

ufdx file • 285, 286

Unallocated space • 10

Updating the signature database (online) • 163, 164

Updating the signature database from file (offline) • 163, 166

Using an offset to jump to a different location in the file • 275

Using the advanced filter • 114

Using the Android Unlock Pattern Carver plug-in • 309

Using the Python Shell • 308, 349

Using the quick filter • 111

V

Verifying hash values • 88, 224

View menu • 346

Viewing image files • 90, 108, 224

Viewing location data on BING • 140

Viewing the Hex data information • 280

Viewing the trace window • 346

W

Welcome tab • 85, 346

Working in data tabs • 90

Working in the Highlights tab • 103, 106, 229

Working in the Project Tree area • 82

Working in the Values tab • 103, 104, 229

Working with bookmarks • 103, 229, 276

Working with carved images • 224

Working with Hex data • 117, 227

Working with Project Analytics • 161

Working with TomTom • 217, 348

Working with watch lists • 78, 123, 348